NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

Congressional Information Service, Inc.
Washington, D.C.

CIS

OVERSIGHT OF COMPUTER MATCHING TO DETECT FRAUD AND MISMANAGEMENT IN GOVERNMENT PROGRAMS

HEARINGS

BEFORE THE

SUBCOMMITTEE ON

OVERSIGHT OF GOVERNMENT MANAGEMENT

OF THE

COMMITTEE ON

GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

NINETY-SEVENTH CONGRESS

SECOND SESSION

DECEMBER 15 and 16, 1982

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
15-720—O WASHINGTON : 1983

S 401-34

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, Jr., Delaware, *Chairman*

CHARLES H. PERCY, Illinois
TED STEVENS, Alaska
CHARLES McC. MATHIAS, Jr., Maryland
JOHN C. DANFORTH, Missouri
WILLIAM S. COHEN, Maine
DAVID DURENBERGER, Minnesota
MACK MATTINGLY, Georgia
WARREN B. RUDMAN, New Hampshire
HARRISON "JACK" SCHMITT, New Mexico

THOMAS F. EAGLETON, Missouri
HENRY M. JACKSON, Washington
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio
JIM SASSER, Tennessee
DAVID PRYOR, Arkansas
CARL LEVIN, Michigan

Joan M. McEntee, *Staff Director*
Ira S. Shapiro, *Minority Staff Director and Chief Counsel*

Subcommittee on Oversight of Government Management

WILLIAM S. COHEN, Maine, *Chairman*

TED STEVENS, Alaska
WARREN B. RUDMAN, New Hampshire

CARL LEVIN, Michigan
DAVID PRYOR, Arkansas

Susan M. Collins, *Staff Director*
Mary Berry Gerwin, *Counsel*
Frances C. de Vergie, *Chief Clerk*
Rachel D. Harlan, *Assistant Chief Clerk*

CONTENTS

Page

Opening statements:
  Senator Cohen 1, 175
  Senator Levin 3

WITNESSES

Wednesday, December 15, 1982

Richard P. Kusserow, Inspector General, Department of Health and Human Services; and Thomas F. McBride, associate dean, Stanford School of Law, and former Inspector General, Department of Labor, accompanied by Frank J. Haendler, project director, Long Term Computer Matching Project, President's Council on Integrity and Efficiency 4

John H. Shattuck, National legislative director, American Civil Liberties Union, accompanied by Norma Rollins, director, New York Civil Liberties Union Privacy Project; Robert Ellis Smith, publisher, Privacy Journal; and Ronald L. Plesser, former General Counsel to the U.S. Privacy Protection Study Commission 77

Thursday, December 16, 1982

Wilbur D. Campbell, Director, Accounting and Financial Management Division, General Accounting Office, accompanied by Edward M. Glagola, Computer Specialist, Accounting and Financial Management Division; James R. Watts, Group Director, Automatic Data Processing, Accounting and Financial Management Division; and John W. Lainhart, Group Director, Audit Operations, Human Resources Division 176

Peter M. Wynn, deputy commissioner for administration, Department of Social Services, State of New York 207

William T. Hogan, secretary, Executive Office of Human Services, State of Massachusetts, accompanied by Thomas H. Spirito, commissioner; Henry A. Cretella, general counsel; John F. Cassedy, director, systems and operations, Massachusetts Department of Public Welfare; and Kermit C. Morrissey, director, external affairs, Executive Office of Human Services, State of Massachusetts 222

David F. Linowes, professor of political economy and public policy, University of Illinois 250

Alphabetical List of Witnesses

Campbell, William D.:
  Testimony 176
  Prepared statement 191
Cassedy, John F.: Testimony 222
Cretella, Henry A.: Testimony 222
Glagola, Edward M.: Testimony 176
Haendler, Frank J.: Testimony 4
Hogan, William T.:
  Testimony 222
  Prepared statement with attachments 233
Kusserow, Richard P.:
  Testimony 4
  Prepared statement 41
Lainhart, John W.: Testimony 176

ALPHABETICAL LIST OF WITNESSES—Continued

Page

Linowes, David F.:
  Testimony 250
  Prepared statement 258
McBride, Thomas F.:
  Testimony 4
  Prepared statement 54
Morrissey, Kermit C.: Testimony 222
Plesser, Ronald L.:
  Testimony 77
  Prepared statement with attachments 150
Rollins, Norma: Testimony 77
Shattuck, John H.:
  Testimony 77
  Prepared statement with attachments 97
Smith, Robert Ellis:
  Testimony 77
  Prepared statement 141
Spirito, Thomas H.: Testimony 222
Watts, James R.: Testimony 176
Wynn, Peter M.:
  Testimony 207
  Prepared statement 216

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Office of Management and Budget, Revised Guidance for Conducting Computerized Matching Programs, May 19, 1982 (47 FR 21656) 265

Office of Management and Budget, Guidance to Agencies on Conducting Automated Matching Programs, April 18, 1979 (44 FR 23138) 268

"Comparison of Office of Management and Budget Guidelines for Conducting Computer Matching Programs Issued May 19, 1982, With Earlier Guidelines Issued April 18, 1979," Congressional Research Service, October 22, 1982 273

Reference Paper on Computer Matching issued by the President's Council on Integrity and Efficiency, November 18, 1982 278

"Computer Applications, volume I, Health Provider Fraud and Abuse," Office of Inspector General, Department of Health and Human Services, July 1982 287

"Computer Applications, volume II, Income Maintenance and Assistance Fraud and Abuse," Office of Inspector General, Department of Health and Human Services, September 1982 339

"Computer Applications, volume III, Federal and State Programs Fraud and Abuse," Office of Inspector General, Department of Health and Human Services, October 1982 361

Description of Project Sonoma, Department of Health and Human Services. Material requested by Senator William S. Cohen, December 15, 1982 392

Letter from Senator William S. Cohen to the Honorable Richard S. Schweiker, Secretary, Department of Health and Human Services, August 27, 1982 394

Letter from the Honorable Richard P. Kusserow, Inspector General, Department of Health and Human Services, to Senator William S. Cohen, September 10, 1982 397

Letter from Senator William S. Cohen to the Honorable Terrel H. Bell, Secretary, Department of Education, October 4, 1982 406

Letter from the Honorable Terrel H. Bell, Secretary, Department of Education, to Senator William S. Cohen, October 21, 1982 409

Letter from Senator William S. Cohen to the Honorable David A. Stockman, Director, Office of Management and Budget, August 24, 1982 415

Letter from the Honorable David A. Stockman, Director, Office of Management and Budget, to Senator William S. Cohen, November 8, 1982 418

"An evaluation of New York State's Wage Reporting System: The Real Costs of Computer Matching," the Privacy Project, New York Civil Liberties Union, December 1982 421

Letter from Stanley H. Torvik, director, Department of Health and Social Services, State of Wyoming, to Senator William S. Cohen, November 16, 1982 442

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD—Continued

Page

Letter from Seth W. Thornton, executive director, Department of Labor, Bureau of Employment Security, State of Maine, to Senator William S. Cohen, November 19, 1982 444

Letter from Kenneth B. Creasy, director, Department of Public Welfare, State of Ohio, to Senator William S. Cohen, November 24, 1982 446

Letter from Larry H. Harrison, chief, Welfare Fraud and Audits Branch, Department of Social Services, State of California, to Senator William S. Cohen, November 30, 1982 448

Letter from Jeffrey C. Miller, director, Department of Public Aid, State of Illinois, to Senator William S. Cohen, December 1, 1982 451

Letter from Noble P. Kheder, director, Department of Social Services, State of Michigan, to Senator William S. Cohen, December 6, 1982 460

Letter from Ms. Dorothy K. Rappeport, Commissioner, Department of Human Services, State of Arkansas, to Senator William S. Cohen, December 6, 1982. 462

Letter from George B. Coleman, deputy commissioner, Department of Income Maintenance, State of Connecticut, to Senator William S. Cohen, December 8, 1982 464

Letter from Donald B. Roark, commissioner, Department of Public Welfare, State of Mississippi, to Senator William S. Cohen, December 20, 1982 466

Statement of Evan Hendricks, editor/publisher, Privacy Times, December 2, 1982 468

Statement of David H. Flaherty, professor of history and law, University of Western Ontario, December 1982 472

OVERSIGHT OF COMPUTER MATCHING TO DETECT FRAUD AND MISMANAGEMENT IN GOVERNMENT PROGRAMS

WEDNESDAY, DECEMBER 15, 1982

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT
OF GOVERNMENT MANAGEMENT,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met, at 9:30 a.m., in room 3302, Dirksen Senate Office Building, Hon. William S. Cohen (chairman of the subcommittee) presiding.

Present: Senators Cohen and Levin.

Staff present: Susan M. Collins, staff director; Mary Berry Gerwin, counsel; Frances C. de Vergie, chief clerk; Rachel D. Harlan, assistant chief clerk; Linda Gustitus, minority staff director; Ed Abrahams, minority staff investigator; and Anne Benson, intern.

OPENING STATEMENT OF SENATOR COHEN

Senator COHEN. The subcommittee will come to order.

In 1977, the congressionally mandated Privacy Protection Study Commission observed that the ability to amass great amounts of data and to sort that data to find the common characteristics of individuals is at the same time the greatest gain and the greatest source of harm stemming from the automation of data systems. More recently, the technological capacity of computers and the widespread availability of computers within and outside Government have made these observations even more important.

It is important that the Federal Government aggressively monitor how well its information policy is keeping pace with its technological capacity. Congress must exercise its oversight responsibilities to determine whether the Government is striking a proper balance between the important concerns of Government efficiency and individual privacy.

Today the Subcommittee on Oversight of Government Management is going to begin 2 days of hearings on the use of computer matching by Federal and State agencies to detect fraud, waste, or mismanagement in Government programs.

Computer matching is the comparison of different lists or files to determine whether identical, similar, or conflicting information appear in them. Comparisons can be made by matching names, social security numbers, addresses, or other personal identifiers.

For example, some Federal agencies match their program files with lists from the Office of Personnel Management to discover whether Federal employees are improperly receiving benefits.

The comparison of records to detect fraud or mismanagment in Government programs is not new. Manual matching has been possible in certain circumstances for years. When done by a computer, however, the process takes on a new dimension. The process is faster and involves hundreds of thousands of records that could not be examined by hand. Thus, technology has enabled administrators and inspectors general to compare records on a broad scale, and, in some instances, to perform these matches as a routine tool to manage their programs.

Recently, computer matching has received a good deal of attention, because of its widespread use by Federal and State agencies. As of January 1982, Federal agencies had completed more than 85 matching programs and State government agencies are now performing approximately 170 matches involving public assistance records, unemployment compensation records, Government employee files, and in some cases, the files of private companies. These projects involve the records of hundreds of thousands of citizens.

The President's Council on Integrity and Efficiency, which spearheads the administration's efforts to reduce waste and fraud in Federal programs, is promoting greater use of computer matching as a management tool by Federal and State agencies. In fact, one of the largest matching programs, being conducted under the auspices of the Council, matches the records of 10 million Federal employees with the files of 15 Federal benefit and loan programs.

The Federal Government is the largest business in the United States. In 1982, it spent over $349 billion in benefit programs, spent over $140 billion in procurement costs, and collected over $621 billion in tax revenues.

With such tremendous amounts of money flowing in and out on a regular basis, the Government would be grossly negligent if it did not take full advantage of technology to insure that it is not being defrauded by either individuals or businesses, and that its programs are as free as possible from errors or waste.

To use technology for these purposes is simply sound business sense, but our desire for efficiency and our fascination for technology should not obscure the very real threat that this "rough beast slouching" toward Washington poses for individual rights of privacy.

What is seen today as an ally against fraud and waste may, unless it is checked, grow into an enemy of the very liberties that we profess to cherish most.

In this regard, the words of three wise men come to mind:

> I believe there are more instances of the abridgment of freedom of the people by gradual and silent encroachment of those in power than by violent and sudden usurpations. [By James Madison.]
>
> The true danger is when liberty is nibbled away for expedience and by parts. [By Edmund Burke.]
>
> The death of democracy is not likely to be assassination from ambush. It will be a slow extinction from apathy, indifference, and undernourishment. [By Robert Maynard Hutchins.]

So it is with this essential conflict in mind that these hearings have been scheduled—to encourage the maximum Government efficiency and to insure proper oversight of technological techniques that are used by the Government.

This morning this subcommittee will receive testimony from two panels of witnesses. The first panel consists of the first chairman and former cochairman of the President's Council on Integrity and Efficiency's long-term computer matching project.

They will discuss the efforts of the President's Council and the inspectors general to encourage and oversee matching programs.

Our second panel of privacy experts will discuss their concerns about the matching programs themselves.

Tomorrow the subcommittee is going to receive more testimony on the usefulness of matching as a management tool and on specific matches that some State agencies have performed. Also we will receive additional testimony on the adequacy of present oversight mechanisms that exist on matching.

I look forward to the testimony this morning, and I expect it will assist us in evaluating the benefits and issues raised by computer matching.

Before going to our first witness, I would like to yield to Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator **Levin**. Thank you, Mr. Chairman. I first want to congratulate you for calling our attention to the problems of computer matching this morning. It has become a common administrative tool. The problem, as always, isn't technology. It's human nature that is behind the use of that technology, and the uses to which it opens the Government.

Technology is wonderful if it is used for proper purposes. It is horrible when used for improper purposes. It can open some doors both to daylight and darkness. We see some examples of the abuse of computer technology in a number of areas.

I look forward to these hearings to determine if we should require some standards, including some cost-benefit analyses, on the use and purpose of computer matching. It is a very complicated area, and I am delighted that our chairman has taken the initiative to bring this problem to the subcommittee's attention.

Senator **Cohen**. Thank you, Senator Levin.

Our first witnesses today are Thomas McBride and Richard Kusserow.

Mr. McBride, who is now the associate dean of the Stanford School of Law, was formerly the Inspector General of the Labor Department and Cochairman of the computer matching project of the President's Council on Integrity and Efficiency. He is accompanied by Frank Haendler, the project director.

Mr. Kusserow is Inspector General of the Department of Health and Human Services and also Cochairman of the Council's computer matching project.

Mr. Kusserow will start.

TESTIMONY OF RICHARD P. KUSSEROW, INSPECTOR GENERAL, DEPARTMENT OF HEALTH AND HUMAN SERVICES, AND THOMAS F. McBRIDE, ASSOCIATE DEAN, STANFORD SCHOOL OF LAW, ACCOMPANIED BY FRANK J. HAENDLER, PROJECT DIRECTOR, LONG TERM COMPUTER MATCHING PROJECT, PCIE

Mr. KUSSEROW. Thank you, Mr. Chairman. I am Inspector General of the Department of Health and Human Services.

I would like to thank the subcommittee for the opportunity to discuss our work on computer matching. This is an activity charged with myth and misunderstanding, and my comments today are designed to clarify the nature and intent of computer matching, and to allay any anxieties about a nationalized data bank or fears of a "big brother" society.

You have invited myself and my colleague, Thomas McBride, to testify on recent efforts by the Federal Government to promote computer matching at both the Federal and State levels of government. In particular, you requested that we address: One, the use of computer matching to prevent and detect fraud, abuse, and erroneous payments in government programs; two, the cost effectiveness of computer matching; and three, public policy issues raised by matching, such as privacy rights of individuals. First, I would like to clarify what we mean by computer matching.

Chart 1, which we brought today, provides a list of terms and definitions that we can refer to throughout the hearing. We generally do not like the term "computer matching." We merely use it as a term of convenience. Just as we perform manual audits to examine and verify data and accounts in programs, we apply computerized programs to examine files to verify the data and identify that which does not belong.

[Chart I follows:]

CHART I

DEFINITIONS

Computer Match: The comparison of two or more computer files to determine similarity or dissimilarity of the data.

Computer Screens: Computer analysis to identify abnormal patterns in single or multiple computer records.

Computer Profiles: Computer identification of variables used to identify potential fraudulent situations.

Hit: Information from two or more computer tapes that appears to be identical, similar, or even contradictory.

Identifiers Used: The key element that is used to identify specific files to extra data.

Matching Data Files: The data files of other State or Federal program agencies which are matched against source data files.

Source Data Files: The data files of the program agency conducting the match.

Mr. KUSSEROW. Computer matching, therefore, is a type of computer auditing technique that includes screening, editing, and scanning data to identify irregularities between lists and files and data within the same list or file. For example, we have compared a list of overdue school loans to health professions with a list of departmental employees and medical professionals receiving payments from the medicaid and medicare programs. When we did this match, it showed that some physicians employed by our Department were delinquent on their loan payments. It also showed that some of the delinquent physicians, who were receiving hundreds of thousands of dollars in medicare and medicaid services, still owed the Federal Government money from their student loans, thus denying other would-be physicians the same sort of assistance.

Now certainly it is irregular for a physician earning large sums of money from our Department to be delinquent on his or her federally subsidized medical loan coming from this Department.

We have also matched death records in the medicare program with social security master beneficiary records to see if payments were being issued to dead people. Dead persons are not entitled to social security benefits.

In doing this latter match, both these programs are within our Department, and yet we found 5,263 dead people continuing to be sent benefits amounting to millions of dollars. Further, we have screened for names of physicians within a program file to determine those who double bill for medicare and medicaid under different provider numbers, without the knowledge or consent of the beneficiary. The purpose of these types of data comparison is to identify the irregularities within a particular data base.

We are really looking at the data base information which is inappropriate and doesn't belong. Once improper information is identified, appropriate verification and investigative efforts can determine whether possible error or fraud exists. The match and subsequent verifications and investigations serve to purify the data base; that is, to eliminate ineligible persons from Federal program beneficiary lists.

We are then free to protect that data from being polluted in the future through front-end editing and/or prepayment screens to verify, for example, eligibility for student loans and benefit programs, or to determine appropriate payment for medical or other services provided to beneficiaries.

An example of how this can work was a program we devised to detect nonissued social security numbers among recipients in the food stamp and aid to families with dependent children programs. From a data base of 2 million recipients, we asked for the identification of all those individuals who were receiving benefits in those programs using a nonexistent social security number. We came up with 5,100 hits. About one-third of these were numbers transposed by the beneficiary in applying for the benefits, or by the program officials when inserting the data into the system. In these cases officials corrected the record for the beneficiaries. The remaining two-thirds of the cases were unentitled or fraudulent.

The next logical step would be to move the detection program to the front end to prevent individuals from participating in a benefit program using a nonexistent number. The major thrust of matching is to move these matching technology points to the front end, with the objective of preventing erroneous benefit payments. Front-end matching is also less intrusive, as its sole purpose is to verify eligibility before payment is made.

Finally, front-end matching is a preventive measure that denies ineligible individuals to divert funds from their intended purpose for the needy, infirm, and the aged. It results in savings, making more assistance available to persons who are eligible under the various benefit programs.

There is also considerable evidence that cleaning up a data base and front-end matching have a deterrent effect. For example, a number of individuals in one State asked that their names be removed from food stamp rolls following a public report of a match of public assistance with State employment and other records. These individuals generally claimed that they had suddenly found work and no longer needed the benefit. This phenomenon of voluntary withdrawal from the program when a technique is announced is more the rule than the exception.

The issue of persons' rights to privacy immediately surfaces in any discussion of computer matching. We take this issue very seriously and have worked hard to protect personal privacy. We have worked with the Office of Management and Budget, as it revised and updated guidelines for computer matching and developed a reference paper to help Federal and State agencies implement these guidelines. Both the guidelines and reference paper are based upon the principles embodied in the Privacy Act of 1974. The guidelines provide for safeguards over how information is to be used, stored, and disclosed. Further, there must be notice to the Congress, OMB, and the public on any matching undertaken by an agency.

Mr. McBride has been instrumental in the revision of the OMB guidelines on matching under the aegis of the President's Council on Integrity and Efficiency and our project. Great care has been taken to assure that they protect personal privacy. He will testify on this later this morning.

The history of this effort with the President's Council goes back to the summer of 1981, when Mr. McBride and I became Cochairmen of the President's Council on Integrity and Efficiency Long Term Computer Matching Project.

Before I discuss the objectives and activities of the computer matching project, I would like to place the concept of matching in its historical perspective. Matching, per se, is not a new concept. Auditors, investigators, and statisticians have been matching lists, file data of all sorts since their professions were born. It is a simple, though rigorous task, necessary to analyze data and information, to evaluate the accuracy of the data, develop conclusions or to establish policy. It is a routine audit process in both the private and public sectors.

As I stated earlier, using a computer to match data is a modern version of an old analytical technique. The advent of computer technology to store and retrieve masses of data have made it possible for us to develop computer techniques, to scan, screen, and analyze that data.

We could sit down and manually look at two sets of data, for example, a list of persons receiving AFDC benefits and a list of persons for whom wages were reported in a given quarter. A manual review of the data would be costly in terms of man-years of work required by the task. By using a computer we can accomplish the same task more efficiently in several man-days. The computer provides us an updated auditing technique to establish common or related items in compared information.

As Inspector General for the largest Department of the Federal Government, as well as the Department that has the largest budget for Federal benefit programs, I am obligated to use the most efficient means available to audit our programs. This must be done to insure that the program dollars appropriated by Congress reach the intended beneficiaries and are not diverted from this goal by fraud, waste, abuse, or inefficiency.

Computer matching, as with generic matching, is not a new practice. We have researched, studied, and continue to evaluate computer matching activities so that we can learn from them and build on best practices.

The first significant computer match of benefit programs I was involved with was conducted in 1976. The Federal Bureau of Investigation matched the employee records of various governmental employees against welfare records in the Chicago area. The results of that match were impressive. There were 4,600 hits—instances of government employees receiving benefits improperly. And subsequent to that, there were hundreds of Federal and State prosecutions that followed.

Senator COHEN. Mr. Kusserow, just for my purposes, and perhaps for Senator Levin, would you distinguish between what's called a "raw hit" and a "solid hit?" Is there a difference?

Mr. KUSSEROW. A hit is the information that we're looking for to come out of a system—the type of information that we would consider inappropriate data that would indicate inappropriate file information. For example, I alluded to a nonexistent social security account number being used by a recipient as an identifier for participating in the program. If we develop a program to identify the nonexistence of such numbers, they would be hits.

Now, these would be raw hits. There could be an explanation as to why there were nonexistent numbers in the file. For example, it could be that the individual applying for the benefit may have transposed the number, or the person, when putting it in the system, may have transposed the number. In these cases they are mistakes, and mistakes can be corrected.

Earlier I gave an example, where in Chicago, we found people that were on governmental payrolls and yet receiving benefits from AFDC. We found we had raw hits in the comparison. However, when we evaluated the data, one of the things that we found was that there are a lot of different reasons why somebody who is employed, could in fact be eligible for AFDC benefits. For example, an employee might adopt a child that has a lot of physical or mental problems which requires a lot of very expensive medical treatment. In such a case there might be provisions for the AFDC program to supplement the employee's income. So the difference between a raw hit and a hard hit is that a raw hit is one that has not been examined as to the causes for the hit without examining the causes for the hit.

Senator COHEN. It could be due to error. It could be a mistaken name, or it could be a transposed social security number.

Mr. KUSSEROW. It could be any number of things, Mr. Chairman. One of the efforts of our particular project is to concentrate on insuring that the data bases are not polluted by inappropriate information. That tends to foul up a system and tends to create hits that are not necessarily a result of fraud or abuse.

Senator **Levin**. Just on that point, quickly, while you've stopped there, how many of those hits, then, were confirmed as being inappropriate from the 4,600?

Mr. **Kusserow**. From that you could split it about 50 percent, and understand we have a gray area.

Senator **Levin**. About 50 percent were people who should not have been on the list——

Mr. **Kusserow**. Were fraudulent in nature. The other 50 percent ranged all the way from people that were entitled to the program to those that had abused the program. For example, we found on the raw hits people that had continued to receive checks 2 or 3 months or 4 or 5 months after they had regained employment. Part of the problem was the delay in the system purging them, and you could not lay that necessarily to fraud. So the hits were good, but they had explanations in them which would make them fall below a screen that would be considered fraudulent by a prosecutor.

Senator **Cohen**. Please continue.

Mr. **Kusserow**. It's from that Illinois project that our own Department of Health and Human Services, picked up and developed what became known as Operation Match, which compared Federal employee files against AFDC and medicaid files.

We ran a pilot in the District of Columbia alone which identified $330,000 in incorrect payments. Because of its initial success, Project Match was eventually conducted on a national scale in 26 jurisdictions. This was by modern standards a very primitive effort. It was overly labor intensive, I think it was probably a little ambitious in scope, there was a question of whether the data was well tested before the results were announced; and it was prior again to the OMB guidelines. There was not any attempt made to really analyze the cost effectiveness of it.

Now our Office of Inspector General for the Department of Health and Human Services continued to improve the techniques of computer-audit applications. We have endeavored to share expertise in computer matching with those tasked with similar responsibilities at the Federal, State, and local levels, and now with the private sector.

We've put together several volumes of efforts to inventory computer applications which we had either previously used or are presently being undertaken to combat fraud and abuse in our programs. This compendium which covers computer applications in the health provider, income maintenance and assistance, and Federal/State areas represents an efficient and accurate means to review the voluminous amounts of data that we have related to the programs they address.

With your permission, Mr. Chairman, I would like to include this compendium of three volumes of our computer applications for the record.[1]

Senator **Cohen**. Without objection it will be done.

Mr. **Kusserow**. In recent years, Congress has passed several laws mandating matching in certain circumstances. Public Law 95-216 enacted in 1977 and effective in October 1979, requires State welfare agencies to use wage information contained in State employment security agency files or social security files in determining AFDC eligibility and payment amounts.

---

[1] See p. 287.

Legislation passed by Congress in 1981 also mandates wage matching for the food stamp program. Effective January 1983 State welfare agencies must match food stamp recipient files with wage information from State employment security agency files or social security files. These legislative initiatives and matching opportunities were the backdrop for the Longterm Computer Matching Project under the aegis of the President's Council on Integrity and Efficiency. This Council was established in March 1981 by the President in order to better coordinate and implement Government policies with respect to the integrity and efficiency in Federal programs. The PCIE is chaired by the Deputy Director for the Office of Management and Budget and consists of the inspectors general and representatives of major departments which do not have inspectors general.

The Longterm Computer Matching Project is considered one of the major projects of the PCIE. Its overall objective is to expand the cost-effective use of computer matching and related techniques to prevent and detect fraud, abuse, and erroneous payments in Government programs, using effective safeguards to protect the rights and privacy of individuals.

The project formed four working groups and a number of subgroups to pursue the tasks necessary to meet the objectives. The four working groups are: matching opportunities, technology and programing, legal and administrative impediments to the use of matching, and State and Federal cooperation. Those are the ones that are characterized on chart II.

[Chart II follows:]

CHART II

LONG TERM COMPUTER MATCHING PROJECT MAJOR ACTIVITIES

Match opportunities: Non-Benefit Matches; Project Clean Data.

Technology and Programing: Standard Data Format; Technical Assistance on Front-End Editing; Inventory of State Matching Activities.

Legal and Administrative Problems: Reference Paper on OMB Matching Guidelines; Seminar on OMB Guidelines; Alternatives for Use of Tax Information; Quarterly Wage Reporting.

State/Federal Cooperation: Incentives and Disincentives; Interjurisdictional Matching.

Mr. KESSEROW. Tom McBride of the Labor Department chaired the legal and administrative, as well as the State and Federal cooperation working groups. We at HHS chair the other groups on match opportunities and technology and programing.

My remarks are limited to the activities for which we were responsible at HHS. The work on match opportunities was established to identify and encourage matching programs and techniques that prevent and detect fraud, waste and abuse in Government programs.

Through its work group, which includes representatives of four States, the District of Columbia, and 22 Federal agencies, we have accomplished a number of significant tasks. Among the key ones is the development and dissemination of computer match programs which identify improper social security numbers. That's what is reflected on chart III known as Project Clean Data.

[Chart III follows:]

CHART III

PROJECT CLEAN DATA/OIG-HHS

Programs identify incorrect and fraudulent SSNS.

Program I identifies any record with an SSN not issued.

Program II detects non-issued SSNS and SSNS being used by person born after the SSN group was exhausted.

Sent to 60 agencies in 40 States, and 4 Federal agencies.

Mr. KUSSEROW. The two computer programs that have been developed in conjunction with this effort have been requested by over 60 agencies in 40 States. This is the one I had referred to earlier where the initial run of it developed 5,100 hits, about two-thirds of which turned out to be fraudulent by nature.

We have also supplied technical assistance in using the programs and are now evaluating their use by the States. The second accomplishment has been our development testing, and use of a number of programs for nonbeneficiary matches. Examples of these programs are included in our volume 3 of the applications, which I'm making available for the record. It sets forth a lot of the nonbeneficiary-related applications of computer technology.

The work group on technology and programing, composed of representatives from five States and 22 Federal agencies, was established to develop standard program data elements and extraction formats and front-end editing techniques.

Basically, our intent here is to raise the level of quality and professionalism in the computer applications to audit problems. The subgroup on standardization of data elements has developed a draft set of compatible data elements and extraction formats to facilitate matches between benefit programs at the Federal, State, and local levels.

These draft data elements have been reviewed by the States and a draft final document will be ready by the end of the month, and I can make that also available for the record.[1]

Senator COHEN. Fine. The record will be kept open for that purpose.

Mr. KUSSEROW. One of the most important accomplishments of this work group is the development of an inventory of State computer matching software packages. The inventory identifies as of October 1982 computer matching conducted by States with labor agencies, the Social Security Administration, and other public and private agencies.

With your permission also, Mr. Chairman, I will make this inventory part of the record.[2]

In addition, the inventory identifies on a State-by-State basis the front-end matching to verify eligibility and interjurisdictional matches between States.

---

[1] The information was not available at time of printing. When received it will be retained in subcommittee files.

[2] The information referred to is retained in subcommittee files.

Before I summarize my comments, I'd like to say a few words about the costs and savings associated with computer matching. We wish we could give you some real hard figures on the cost benefits of matching nationwide, but that's not possible at this time for several reasons. The State and Federal agencies have generally included the costs of matching in total data processing costs rather than breaking them out, and the followup on hits associated with many matches has not been completed. Therefore, we don't know the exact extent of recovery as a result of the matches.

But one of the purposes of this inventory, which we introduced into the record, is our first major effort to begin focusing in on Federal, State and local agencies to start developing the kind of data that will enable us to make an effective review of the cost effectiveness of these techniques. We are cognizant of the need for further documentation of the cost benefits of our activities, and this will be a continuing part of our effort in the future.

We are convinced, however, that matches recover far more money than they cost. For example, the State of New York has been matching welfare recipient records with quarterly wage reports from New York employers for several years. They estimate that they will save $114 million for the period 1979 through 1983 from the systems cost of $28.1 million. This is roughly a 4-to-1 return on the dollar.

In 1981, California matched State income tax refund records with files on recipients ordered by the court to repay the payments from the AFCD program. The cost was $6,000 for a recovery of over $200,000.

Our own Project Spectre, which matches social security benefit payments with medicare death files, has led to $7½ million in recoveries to the social security trust funds. The recoveries in this case cover all moneys collected by our investigation including checks not cashed but given to the Treasury.

[Chart IV follows:]

CHART IV

PROJECT SPECTRE/OIG-HHS

Matched Death Files in Medicare and Medicaid to Determine Beneficiary Payments to Deceased Individuals.
8,300 "Raw Hits" Obtained.
24 Convictions; 62 Indictments.
5,263 Persons Terminated From Program.
$7,605,218 Recovered For SSA.
$25.2 Million Saved.
$108 Costs Per Investigative Case.
$4,788: Savings Per Investigative Case.
$1,065: Recoveries Per Investigative Case.
$44.00 Saved Per Every $1.00 Spent by OIG.
$9.90 Recovered For SSA Per Every $1.00 Spent.

Mr. KUSSEROW. We project that the total savings potential there could reach $25.2 million. This does not include any of the cost avoidances for the future that would arise from the fact that the 5,263 people who are dead are eliminated from the files and will not be getting additional money.

Another example of this continuing benefit that we did taking master beneficiary records of the social security death files and matching them against the black lung program. We came up with another $12 to $15 million.

And what was really startling in that situation was the average period of overpayment for people that had died was 81 months past death. So what we have done is to eliminate from the files those payouts which, if were not eliminated, would have continued to be paid out as the cost of the program continued to go up.

These are just a few examples of the potential savings from that experiment.

To conclude my testimony, we are stressing the positive aspects of computer matching. Matching is a computer auditing technique used to verify information in a list or data file, and to purify a data base so that, for example, dead people don't receive checks and bad data don't lead to poor services.

Therefore, by purifying the data base we have money available for services to those who are eligible for Government benefit programs. I'm convinced that matching is a cost-effective tool for insuring the integrity of Federal programs.

I hope my comments on computer matching have been helpful, and I thank you for the opportunity to allow me to make this presentation today.

Senator Cohen. Thank you very much. Mr. Kusserow, before we get to questions, we'd like to have Mr. McBride present his testimony.

Mr. McBride. Thank you, Mr. Chairman. It's a pleasure to be here, and I think that congressional attention to this issue, as you noted in your opening remarks, is very timely. These are major legislative issues not only in connection with the mechanics of matching, but in connection with privacy and other issues, which you touched on.

The genesis of computer matching is not all that mysterious. It has been a predicate of most of the large government programs, that the administrators of those programs, whether they be Federal or State, are enjoined to verify the eligibility of those who apply for benefits. That eligibility may depend on income. It may depend on status, age, dependents, and so forth.

What we have found with the mushrooming growth of Federal programs—and I think, as of a 1980 tally, there were 58 federally funded programs dependent in some form on income eligibility—that the machinery for verification was simply inadequate and ineffective to assure that those receiving the benefits were in fact entitled.

In many of the programs, the servicing organizations, particularly at the State level, were so understaffed that the programs became little more than a self-certification exercise. If you put the right things on the application form, you got the benefits with only minimal attempts to verify.

It is a logical outgrowth, I think, of the installation of inspectors general in the various major Federal agencies, a statutory initiative in which this committee played a large part, that they would focus on this problem. We were instructed by congressional action to go after fraud and waste in Federal programs, and this was one of the most obvious, and probably the largest, dollar item.

I was appointed in 1977 as Inspector General of the Department of Agriculture. In looking at the programs of that Department, it became immediately obvious that the largest program was the food stamp program; and, there was, at least by newspaper accounts, a significant volume of fraud in that program.

We began to do some tests, first in the southeast region of the United States, looking at the food stamp rolls and matching them against wage data. I'd like to say a word about wage data because that is critical to the whole computer matching exercise.

Wage data in 40 or 41 States are reported quarterly by employers to the State employment security agency, essentially for purposes of assuring eligibility for unemployment compensation benefits. And that wage data is, by and large, accurate, and, relatively speaking, timely; that is, it is reported quarterly and almost immediately available thereafter.

It is also, I think, important to realize that matching in the unemployment insurance program was probably going on back in the 1960's, certainly manual matching was going on, to determine whether those applying for unemployment compensation had the proper quarters of contribution and, indeed, were not employed at the same time they were receiving benefits.

With the advent of computer technology, it was only a logical management step to do it by computer. And in the early 1970's, there was quite a bit of matching going on at State levels, largely unnoticed by Federal oversight.

I took a look at the food stamp program, and what we found was that a substantial percentage—and, indeed, the largest single percentage—of what was called the error rate in the food stamp program was due to either underreported or unreported wages. We came in the southeast region with literally thousands of hits and millions of dollars in recoveries, and, more importantly, many millions of dollars in costs avoided by termination of benefits to ineligible people.

That exercise convinced me that this was an extraordinarily cost-effective tool. It also convinced me that it should be applied to other Federal benefit programs. It also convinced me that the administration should take some sort of leadership role in pointing out the value of this technique to Federal and State agencies who were not employing it.

It also, I think, pointed up the need to take computer matching techniques and install them as part of routine program management. It's not something that the auditors or the inspectors general should be doing. It's something that those charged with the accountability for the expenditure of funds should be doing as part of their routine program management.

Mr. Kusserow referred to the front end. That's where the real prevention and real savings should occur. When someone applies for benefits, there should be a check to see whether they in fact have reported their earnings or whether in fact they are secretly employed.

The collateral issue, of course, was—and still is—a fairly widespread public perception that some of these programs are riddled with fraud. And while there may be much exaggeration in that public perception, there is enough fraud to give one pause. And the reputation, if you will, that many of the better social programs that the Congress has enacted over the years could suffer and the programs themselves could be jeopardized unless there's a reasonable level of guarantee of program integrity.

Matching allows us to do that to a great degree. I have been beating the drums for a computer matching project going back to 1979 probably. When the President's Council on Integrity and Efficiency was formed, I finally found that there was an administration interested in how computer matching, with privacy safeguards and other safeguards, could be encouraged.

The computer matching project does not run matches. I think that is a very important point to get across. As cochairmen of the project, Mr. Kusserow and I have not been running matches. We may have been running them wearing our Inspector General hats at HHS or at Labor or at Agriculture, where I was before, but our basic objective was to make sure that legislative, legal, and regulatory obstacles were cleared away; that due attention was given to data safeguards and privacy safeguards; and that legislative issues that attend on the match exercise were surfaced.

I think there are two or three critical issues. Congress has, as Mr. Kusserow noted, required matching; in the AFDC program, required wage matching, and in the food stamp program. And I think these actions, while commendable, have not been taken in the context of the overall impact of computer matching as a tool in terms of guaranteeing the integrity of these programs.

One of the big issues is wage data—assuring that we have access to the wage data, and taking initiatives so that the 12 States that are not conducting quarterly wage reporting programs do so, because the dollar savings are immense. Mr. Kusserow has mentioned, for example, the New York example. I believe Peter Wynn from New York State will be testifying here tomorrow.

I won't go into the cost-benefit details of that effort, but in that State, in New Jersey, and in a number of other States, the effectiveness of matching quarterly wage data has been proven time and time again. And the savings far outweigh the costs. But it is a legislative issue that I think the Congress should deal with. Should the 12 nonreporting States be brought into a quarterly wage reporting system?

Second, and a far more controversial issue, is the question of access to tax data. Here, I think, you must be very precise about exactly what you are talking about. There is a tremendous volume of tax data, ranging from charitable deductions, alimony, wages, dividends, interest income, some of it supplied by the taxpayer, some of it supplied by third parties such as banks and savings and loan institutions. And depending on what kind of data you want and what program purpose you want it for, you may get a different legislative answer as to whether it should be available for computer matching.

So I think precision, when you are talking about IRS files, is very important. And the debate up to this point has suffered from imprecision. On the one side, one camp would drop an iron curtain around all tax data and the other camp would be portrayed as desiring full access by all Government agencies at all levels to all tax data. Neither, to me, is a wise solution.

There is a balancing between the potential cost benefit of the data, the program integrity purpose for which it is desired, on the one hand, and the invasion of privacy or confidentiality on the other hand.

Finally, I think a major issue is the social security number itself. It has been referred to as not a national identifier, and yet incrementally it has become used as such. Most of us have it on our driver's licenses, on our tax returns, on our savings accounts, and it is very close to being a national identifier.

The computer reads numbers basically, or letters translated to numbers, and the social security number has been the basic data element that opens the door to the computer file. You match the social security number and from there you match wages and whatever else that is in the data base.

I think addressing that issue of just what the social security number is supposed to be in our society is a legislative issue, attention to which is overdue. It's those kinds of issues that the computer matching project has been addressing.

We have also been addressing the issues of technology, how you do matches, how you do them in a cost-effective way, how you use screens and the other sophisticated techniques.

We have also been addressing the question of interjurisdictional matches. It is not uncommon, of course, for one bent on fraud to get AFDC or unemployment or food stamps or other benefits from more than one jurisdiction simultaneously. And given our Federal system, there are little incentives at this point for interjurisdictional matching. Where those have been done, for example, in the unemployment insurance program, they have rendered high payoffs in terms of recoveries and cost avoidances.

Turning to one of the more fundamental concerns of the committee, the privacy concerns, I think, first off, that it's not a black or white question. I think all would agree that we want to take all reasonable steps to insure the integrity of these programs. I think all would agree that we don't want a national data bank on which all information about every citizen in this country is compiled in one massive dossier.

Computer matching does not create data, or if it does, it's only in the most temporary way for purposes of identifying hits and verifying. The data is already there. I think in many ways there is no turning back. That data is going to be there, and the volume of that data is going to grow due to the varieties of programs, the variety of benefits, and the population growth of our country.

The question is how that data is used and how it is safeguarded. Computer matching in many ways is less intrusive than some of the verification techniques used in the past. I remember when I came to Agriculture it was on the heels of a large debate about the practices of certain Southern State's welfare agencies, of aggressively going out and actually surveying households to find out if there was a man in the house.

Those are the kind of privacy intrusive verification techniques that, to my mind, pose a greater threat than computer matching.

Senator COHEN. Of course, under those circumstances, there is also a greater chance of detection by the people being watched in cases of illegal surveillance or harassment. In matching programs, if people don't know that they are being surveyed or even, indeed, conceptually grasp that their profiles keep popping up in the computer——

Mr. McBride. Well, the OMB computer matching guidelines and the Privacy Act do require publication, public notice to Congress and others of these match uses. I am not sure that most welfare recipients read the Federal Register, and I would myself advocate wider public notice.

Senator Cohen. I'm going to mention that in the questions, too, because the OMB guidelines also requires that a notice be published in the Register, and that OMB and Congress be notified specifically.

I was wondering why there is a requirement that the Congress and OMB be notified. I assume because Congress and OMB don't read the Federal Register. [Laughter.]

Mr. McBride. I think that even the notices that go to the Congress especially may not be read in every instance. But the widest possible public notification of this technique is desirable, and I see nothing wrong with putting it on the application forms that this information will be verified; your wage, income, and other information will be subject to verification, including verification by matching computer data and other sources; maybe even referring to the specific sources. That is fairness.

It does seem to me that we should expect that those applying for Federal or State benefits, whether they are welfare benefits or unemployment benefits or whether they are Government loan benefits, should be subject to this kind of verification. When I file my Federal income tax every year, I am aware that my bank or savings institution is sending what is called a 1099 to the IRS that tells them how much interest or dividends I was paid during the year.

I have operated on the presumption that, at least on a sampling basis or a test basis, the IRS conducts computer matches to make sure that I'm not cheating on my taxes. And I think that's fine. It's a proper management compliance safeguard.

I think that same degree of verification should be imposed on those applying for or receiving benefits from a number of Federal and State programs, but I do agree that notice is a fundamental tenet of fairness in this area.

The computer, however, is less intrusive, if you will, than manual matching. One, it is only looking for one item of data, whatever it is programed for—wages or interest income or whatever it might be. It is not wandering through a file looking into other confidential data and retaining it, as the human mind would inevitably do where it looking at the same files. So in many ways the automation of the computer itself is a privacy safeguard.

Senator Cohen. If I may just interrupt for a second again, what about profiles? For example, there is one that we will discuss a little bit later, the so-called welfare queen. I don't particularly like the term, but what would be a profile of a welfare queen, for example?

Mr. McBride. My guess would be that you would be looking for, one, numbers of dependents, large numbers of dependents. You might be looking for age group. I don't know if there is a historical basis of who the welfare queens are, whether they fall into any age category.

You would probably be concentrating on interjurisdictional matching because the welfare queen pattern typically is to get benefits in more than one jurisdiction.

We have used that kind of profiling, for example, in the Federal Employees Compensation Act area. Those are the people who receive Federal disability pay. We developed a fraud-prone profile of people—people of the working age group under 60—I forget what the age cutoff was, type of injury, lower back being the most suspect; and we culled out, according to that profile, a volume of *x* thousand people from the rolls.

There were 47,000 people receiving Federal employee disability compensation. Of those, we found a distressingly high percentage who were in fact working while receiving 100 percent disability, and that disability pay of course is something like 70 percent of their regular salary and tax free.

Senator COHEN. There are two points I want to make in respect to this.

First of all, it is not the computer just looking for one thing, such as income data or wage data. The computer takes into account a whole range of factors, such as the age of the individuals involved in disability payments. It might take into account the number of children. It might take into account income levels and other Federal programs that they might have. It might theoretically take into account race.

It might be, for example, as I was told at a hearing some time ago, that the Federal Government had come to the conclusion that there was less likelihood that students coming from a low-income family would repay their loans, which I took fairly strong objection to. The profile would contain a whole series of factors, not just wage base.

Mr. McBRIDE. That is true. You can program it, of course, to look for any item of data. You could go through the IRS returns and find out who is paying alimony or who has submitted psychiatrist's bills for medical deductions or all sorts of things, things that are in most instances irrelevant to any bona fide management purpose.

Senator COHEN. That was one point.

Second, it is the wrong subcommittee to bring up the issue of disability payments.

Senator Levin and I have worked for many months to try and deal with the very serious problem of social security disability payments. We have profiles that have been developed by computer, and disability payments that have been discontinued with no human contact coming about until such time as those cases are appealed to an administrative law judge. Two-thirds of the cases appealed are being reversed.

So, I want to discuss this later, but it presents problems when you are dealing solely with computers and there is no human element involved.

Mr. McBRIDE. I do not think it is legitimate, however, to let the computer matching program bear the burden for poor administrator judgment, and that has happened, there is no question. That could easily happen, and indeed has happened, without any assistance by the computer.

Verification of hits is essential. That is the risk of computer matching. The computer does not think. It matches. And if there is an error entered, you will get an error out. And any administrator who terminates benefits or sends notices of termination based on hits without further verification is doing a disservice to the program. And there have been instances of that.

Indeed, in the earliest Project Match one of the problems was the premature publication of raw hits, creating a public impression of a volume of fraud which far exceeded the reality.

That is why, I know in my own matching programs in Agriculture and Labor, I try to be very careful in, one, verifying the hits and only going public when we had actually done that verification and knew we were dealing with a population, if not totally of fraud, at least of clear overpayment, whether due to error or fraud.

Senator COHEN. Are you familiar with the Massachusetts case?

Mr. MCBRIDE. I read it in the paper. I was going to mention the Massachusetts example.

If the newspaper accounts are correct, that seems to be another example of what I would call premature human determination of ineligibility, based on what may be faulty data.

The computer gives you a lead. That is all it does. And it is up to human beings, program administrators, then to verify that, and they should not take any action, in my view, until it has been verified.

I mentioned the necessity of addressing some of these legislative issues, and I will use another example to point up what I think is the urgency of that, which also relates to SSI disability, an issue I am sure you are intimately familiar with, more so than I.

That was the effort to have recipients sign a waiver granting access to tax returns. The initiative, in a sense, was commendable. Program administrators were trying to insure eligibility and guard against fraud. But the absence of congressional authority for accessing the tax data put the program administrators in the posture of having to go behind the barn and get the data by questionable means.

I think it is far preferable that Congress address the cost benefit, privacy, and other issues attendant on that and say, "Do we want, for SSI disability recipients, to have the program people have access to certain elements of tax data to verify?" If there is a legislative "Yes," then program administrators can do it. If there is a "No," they can't.

I think it is unfair to castigate bureaucrats for poor management of the program and not give them clear legislative signals on what the parameters of permissible verification are.

The data, once obtained, generates hits. As I just noted, hits have to be verified, and I think no administrative action should be taken until that is responsibly done.

And then the other data, the non hit data, the unverified hit data, and indeed all the data that you have gotten from the hits, once you have your leads and have verified them, you destroy the remaining data. That is it.

There is no data bank, no permanent bank. There is no file or anything else. What you have done is generate your hits and you have gone on to investigate, verify, and terminate benefits, prosecute, or take whatever action is necessary.

The legislative issues that I mentioned—expansion of quarterly wage reporting, the difficult question of access to certain elements of IRS data for certain program purposes, the use of the social security number, and the compatibility, not only with the Privacy Act but with larger concepts of privacy—are all ones that I think the Congress must address.

And, as I say, it is very much a balancing test. Cost effectiveness and cost benefit is probably the most important factor, other than privacy, that weighs in that balance.

I would like to say a word about cost benefits because it has been a rather elusive concept to get hold of. Cost benefit, in terms of how much it costs to do the match versus what you get from it, is almost always overwhelmingly in favor of doing the match.

That comes from the nature of the costs of automation itself. If the data base is clean, and the elements match in a data format way, it may only cost a few hundred dollars to match thousands and thousands of names.

So you are always going to get, even if you recoup only $5,000, $10,000, or $20,000 from a match, you are almost always going to repay the cost of doing the match. And a lot of our cost-benefit thinking has focused on that, and I think that is important because if you invest 5 cents in additional program management costs to insure or verify eligibility and you get $1 return for every 5 cents spent, you say, "Hey, that is fine. That is good management. That is the way we want these programs run."

If you are looking at it from a privacy point of view, where you say, "Well, we are matching 5 million records, and we are getting 25 hits," then that is a different cost benefit. The dollar factors can't be pinned down, certainly, when you are talking about privacy.

Also, I think you have to keep in mind program size, and that is one I have tried to get some data on, but it is very, very difficult. The hits, the overpayments, for the big benefit programs run somewhere between 1.8 up to maybe 4 percent, depending on what program you are talking about.

For AFDC, the hits are probably somewhere at the lower end, because they do a little better job of verification. Food stamps is a little higher. Unemployment insurance may be even higher, in some States particularly.

I would estimate—and this is something that I was hesitant to do and never did when I was an inspector general, but now I am enjoying my new-found academic freedom—I would guess that, looking at one-time recoveries and savings, if you were to do wage matching on the biggies—AFDC, food stamps, medicaid, the housing programs, unemployment insurance, maybe worker's comp—you would probably come in with about $2 billion or more in potential recoveries and savings. That is kind of a one-time shot. In addition, you would have to estimate future costs avoided.

The other element in cost benefit is the preventive and deterrent element. You save all this money one time, but you also save an awful lot of money because people who otherwise would continue on the rolls aren't continuing. So the next year and the year after and the year after that, you are also saving money, but that's hard to measure.

You are also deterring people. I recall when we did our food stamp matches in Birmingham and Memphis, there was a drumfire of local publicity, not generated by us but by State officials, about the match, and the volume of hits we were getting from finding people who weren't reporting their wages. There was a sudden heavy volume of calls or walk-ins to the welfare office saying, "I want to be terminated. I just found a job." The deterrent impact was apparent from that kind of match.

So cost benefit has many different angles at many different levels, some of it quantifiable in dollars, some of it not.

I think that those doing matching are increasingly aware of the desirability of keeping some kind of record of basic cost-benefit factors—at least how much it costs to do the match, how much was recovered, costs avoided from doing the match and its proportion to total dollar volume of the program.

I would like to note that there is a lot of matching going on, and a relatively small volume of it is directly Federal. Some of the more highly publicized examples, such as the VA loans, the Federal Employee Compensation Act that I mentioned, the black lung death file, those have gotten a lot of print and saved a lot of money, but they represent, numerically, a relatively small number of matches—30, 40, something like that.

My guess is that there are routinely going on at State levels in the unemployment insurance programs about 200 routine matches, going on all the time, matching people who applied for benefits versus wage records, or interjurisdictionally between States.

If you look at matches involving other programs, the welfare-type programs, I would guess there is another 200 or 300 more. So my guess is we are talking about a population of roughly 500, more or less, routine recurring matches going on, some of them subject to Federal legislative action, some of them not.

For example, the States' general assistance programs have the same management problems as AFDC, and there is no Federal jurisdiction over them, and whether or not to use matching is the State's business. So whatever the Federal action may be, some substantial volume of State matching will undoubtedly continue because it is a proven cost-effective management device.

I have no further particular comments but would be delighted to respond to any questions you or Senator Levin would have.

Senator COHEN. Thank you very much, Mr. McBride, for the very thoughtful testimony.

I would like to say at the outset that the purpose of these 2 days of hearings, that we intend to continue next session, is not to reject matching as a concept or the computer as a management tool for discovering fraud, mismanagement, and waste. The "third wave" is here, and I think we cannot deny its existence.

The real question is whether we are going to fall down and pray to a false god in a sort of idolatry. We will look at efficiency only—if that becomes the standard—to which we then fall down and pray. It seems to me that we forget something very important in our society.

I spent many years prosecuting criminal cases and many more years defending criminal cases. As a prosecutor, I came to the conclusion that at least 95 percent of the people I was prosecuting were, in fact, guilty. I got the same impression when I was defending individuals.

Nonetheless, we don't strip away our constitutional protections of due process by virtue of the fact that we have a predisposition to a certain conclusion. We safeguard those sacred liberties, and that, to me, is what is involved here. And you point that out.

Second, there is a question about an element of unfairness in the approach of the so-called computer matching today. We are focusing on AFDC, unemployment benefits and those areas in which people seek Federal assistance at the lower end of the income scale.

In fact, Senator Levin and I have spent several years now trying to investigate fraud and waste at the Federal contractor level, in which we have found millions of dollars being wasted in Federal contracts. We found that agencies did not share their information; thus, one contractor who had been guilty of fraudulent practices, or who had been debarred by one Federal agency, could walk across the street to another agency and get another contract. No record was being maintained by the Federal agencies, and there was no apparent intent to maintain that kind of a record. In matching there has been a focus upon the low-income scale of our society and none on some of the more major fraudulent practices involving hundreds of millions of dollars that also take place.

Mr. McBride. May I comment a moment on that, Mr. Chairman?

Senator Cohen. Sure.

Mr. McBride. That has been a concern of mine as well, not only the reality, but the perception that this will be perceived as some antiwelfare recipient drive exclusively. There have been quite a number of matches, and indeed, some of the most cost-effective exercises have involved other Federal benefit programs. One of the first ones which I did at Agriculture involved matching the SBA and FmHA disaster loans. It is not a large loan program, but I think we came up with something like 250 verified hits that saved somewhere between $1 and $2 million, or recovered that amount in loan funds. Basically, people were applying for loans from both agencies, when they are only eligible for one, and they were taking both.

I am told that the recent highly publicized NASA Inspector's General investigation of contract fraud and abuses by Rockwell used computer matching techniques to look at billings. In that case, a somewhat intricate exercise involved fixed price billings versus cost-plus billings, and found out that the Government was being overbilled.

Computer screening and profiling has been used heavily in the highway contract area. You've probably followed the accounts of wholesale bid rigging in the Federal highway construction program. Computer patterns of successful bidders, county by county, generated the leads which led to many of those investigations.

And of course, you have a very large population of people who borrow money from the Government, some of whom may be low income, but many of whom aren't. Things like the medical education loans, VA loans, and so forth. So there has been a quiet growth in the application of these techniques to nonwelfare programs. There will always undoubtedly be a larger volume of verification in the welfare programs, because of the large volume of recipients and dollars, but I agree with you that this is not a technique which could or should be limited to those programs.

Senator COHEN. There is a point I want to make before coming to the general questioning.

You mentioned the issue of deterrence. I suppose we could have a requirement that anyone who seeks Federal assistance would be required to sign a release or waiver of their Federal and State income tax returns, and then this information would be made a part of the record of all Federal agencies and State agencies. That would be a very sufficient deterrent to preclude people from even wanting to seek Federal assistance, I assume. So you have that problem as well, you can make a very effective deterrent by forcing the release of information which would otherwise be very confidential.

Mr. MCBRIDE. I would not advocate that.

Mr. KUSSEROW. I just wanted to add to your observations earlier, Mr. Chairman, concerning two things. The first is: How well are these computer applications designed so that they be least intrusive? I would point out that that is one of the major thrusts of what we're trying to do through the computer matching project is to upgrade quality, so that you don't have a situation where you are going all over the map. But you are pinpointing exactly what is needed and no more. The second thing is, if you are concerned about focusing in on the beneficiary side, the major thrust of what we are doing in our Department is just the opposite.

We feel that the beneficiary programs have been pretty well identified, and as indicated in the three volumes that we have made available to you, a compendium of what we are doing, you will notice the second volume, the thinest, is the only one that relates to income maintenance programs. The other two, particularly the first one, which is on health provider areas in medicaid and medicare, the entire focus is on the provider's side—the physician and his double billing, using different provider numbers, the pharmacist who is charging a name brand drug, when he is issuing a generic, and things of that sort.

So the major focus right now—one of the things we are trying to do is to move people beyond the very primitive matching of lists into much more sophisticated types of efforts, using computers. For example, in volume 3, we identified instances where the cost of equipment was charged, as direct expense to the program, but should have been included in the administrative costs, which sounds awfully technical, but in terms of costs to the Government, is a very important feature. So we are very much aware of the fact that we need to move on, and your concerns are our concerns, as well.

Senator COHEN. Thank you very much, Mr. Kusserow.

In your statement, you say that you and the President's Council want to allay fears of a national data bank and of "big brother." In its 1978 annual report, your office listed the lessons it had learned from Project Match. The report stated "This underscores the importance of a national recipient system, under which a central data base will be kept current for all AFDC recipients nationwide."

Then later in 1981, HHS proposed the system of a similar system to Congress, under which the Secretary of HHS can request other Federal agencies to contribute appropriate information to the central AFDC file.

Now what do you mean by "national recipient system" under which a central data base would be kept current?

Mr. KUSSEROW. That was issued prior to my coming, but let me think, and see if I can put it this way: AFDC is a federally funded, State-administered program. So what we have is 50 different systems operating off the same program dollar. I think what they are trying to address in that 1978 report is, how do you establish better communications between these 50 different jurisdictions? So I think that what they're talking about is communication between different AFDC programs, all embarked on the same Federal program, but in 50 different jurisdictions.

But the idea is to take out the barriers to allow them to do better jurisdictional matches or communicate among themselves, so that you will not have a situation where people might be sitting in an area where they were a spit and a holler from one State border, and go collect benefits from different States.

Senator COHEN. Aside from what you call it, what's the practical effect? You say you take down these barriers. I was going to ask you, Mr. McBride, about a point you made in your statement. In your printed testimony and also in your oral remarks, you referred to the obstacles that prevent better computer matching techniques—obstacles that exist currently. I was wondering why the term "obstacles" was used, as opposed to, for example, legal restrictions that reduce the availability of matching?

Why would the Privacy Act be seen as an "obstacle," or why would the Constitution or some other legal requirement be termed an "obstacle," as opposed to a congressionally sanctioned prohibition or restriction against the availability of matching data? I want to use that in a context of a central data base being kept on AFDC recipients.

Mr. MCBRIDE. Let me comment on both areas.

On the central data base, my own view, with having had some exposure now to the variety of Federal and State data bases in this matching exercise, is that privacy considerations aside, it is a foolish idea, because the data would be so voluminous, the data would be so late, State compliance would be so spotty, and the errors would be so many, that it would be a nightmare, just in terms of the practicality of it, leaving aside any political or ideological issues.

On the other issue you raised—the obstacles—the obstacles tend to be of a wide variety. Some are legislative in the sense, for example, that 12 States do not have quarterly wage reports. In those States, you can't get timely wage data, and you can't do this wage verification. That to me is an obstacle. That is a statutory obstacle. It could be overcome by legislative action.

There are also obstacles in terms of data compatibility. For example, the Federal agency or even the State will keep its data one way, or by regulation, may even be required to keep its data one way. For example, the rent subsidy programs of HUD don't require social security numbers, so you can't match them. That is the only practical way you can access that data.

Those tend to be administrative impediments or obstacles, which are remediable, and by administrative action. There are a variety.

Senator COHEN. You recommended some changes in the Privacy Act. Is that act an obstacle?

Mr. McBRIDE. It has not been. I am not a privacy law expert, and I was not involved in the work of the Commission or the congressional action leading to the passage of the Privacy Act, but I have always been somewhat baffled by what seems to me to be a somewhat illusory protection, the routine use clause of the Privacy Act. Basically, what those conducting matches have done, those subject to the Privacy Act, is to publish notice and add the match as a routine use, even though it did not seem to have a clear nexus to the purpose for which the data was originally collected.

For example, the OPM personnel files or departmental payroll files, as a routine use, you match it against student loans. That certainly wasn't the reason they collected the OPM file, but you publish a routine use notice, as a predicate to matching.

So to me, the Privacy Act has not been an obstacle, but I've often been puzzled as to whether there is some distortion of the intention of the legislation. Routine use has become pro forma.

Senator COHEN. You mean distortion by the agencies, saying that, "Yes, it is a routine use that we're collecting this information for," not by the Congress in passing the law itself.

Mr. McBRIDE. No. I've just been baffled by it. Obviously, I think that most of these uses that we have applied in this fraud prevention program are proper uses, whether they are proper routine uses within the meaning of the Privacy Act, I would question. So I think some legislative attention should be given to developments in that routine use area, since the passage of the Privacy Act. We should have some better definitional guidance.

Senator COHEN. I have just a couple more questions before I yield to Senator Levin. The problem involves not only issues of due process or unreasonable invasion into privacy: that's a fairly illusive concept there, even as it's defined by the Supreme Court. The question is, who is overseeing these computers? You mentioned information being collected for which it might not be a routine use and yet retained in files to be cross matched with some other program. The question is: Who is overseeing this information? OMB has not had a very intense interest in oversight of computer matching. In fact, they want out. They wanted to pass that on to the Council on Integrity and Efficiency. But I think that says something about who is watching the machines or who is watching the programs.

Mr. KUSSEROW. Mr. Chairman, I would like to say in part that I would hope that we in the inspector general community are looking at the machines, because one of the major purposes of these computer applications, as we are developing them, is to really use the computer.

For example, in the simple case where you have people receiving checks, there isn't anyone in this room who doesn't know somebody or know an instance where somebody tried to get the check to stop coming. Like the credit card companies, when something comes into the system, you can't seem to stop it. We have an obligation in the inspector general community to take those machines and make them do what they should be doing. By devising special programs we take steps to automatically eliminate problems which cause erroneous checks to be printed. In the vast majority of cases where checks go out to dead people there is no fraud. Rather the checks were printed, sent out, and someone was just picking them up. So I would have to say that that is part of our responsibilities, to start taming those machines and make them do what they should be doing.

Senator **Cohen**. You see, one of the problems is notice. And that's what stuck in my mind when we talked about the sort of surveillance being conducted. I suggested that perhaps there might be a better method than to have a computer scanning its own brain waves, as such, to retain or gather information unbeknownst to the individual or individuals on a massive basis.

Then they said. "Oh, we have got to have notice." We used to have notice by forcing the requirement before the computer matching could be done. Now we have changed that. Among the guidelines we've said, "You don't have to do that." You have to publish notice that is reasonably close in time or proximity to the actual match.

Now a match was done, as I understand it, in August of this year, dealing with student loans. Is that correct? Are you familiar with that?

Mr. **Kusserow**. That's over in Education.

Senator **Cohen**. Well, let me tell you. It was done in August. The publication in the Federal Register came out in December. Now would you say that is a reasonable notice of 4 or 5 months after the computer match was done?

Mr. **McBride**. I don't think either is reasonable, because, as I said, earlier, certainly, students borrowing money at Stanford don't read the Federal Register before signing a loan application. If you're going to give notice, put it on the application. Advise the borrower that the eligibility would be subject either to verification by computer matching or for subsequent collection action.

That's fairness. Put it somewhere where the applicant can see it. Many of the forms do tell them that the agency will resort to a variety of means to verify eligibility. So I think that most applicants are not under any illusions that there is not going to be an effort made to verify their eligibility. Whether you want to go further and specify the exact modes of verification you are going to use may be going too far.

On the income tax form, interestingly enough, it doesn't have any such notice. Yet, there's probably more matching going on by IRS itself than anyplace else.

Senator **Cohen**. My concern is that we not simply allow this "third wave" to overwhelm us and become indifferent to it, that we start changing guidelines, that we start dropping the notice requirements, that we stop requiring the proximity notice and the intensity notice that's required, and suddenly say, "Well, the computer is here. By God, you're going to be on notice. If you're going to do business with the Federal Government, they've got everything accumulated in Washington, and they're going to get you."

Once we become amenable to that sort of mind set, then, you know, we're really not too far from "1984," because "big brother" is there and everything is accumulating. I guess it cuts at the heart of our system, also.

We haven't gotten into IRS yet, because we do make exceptions about making that information accessible to other agencies now. But the IRS has always depended upon voluntary payment by the citizens, assuming and presuming honesty.

If we start changing that presumption and allowing it to settle into our mind set in our society, then we have, in effect, a totalitarian type of mentality that is situated right here in Washington. We could no longer depend upon the honor system of people voluntarily paying their taxes, because they'll hold back or they'll just fear that all this confidential information is going to be widely disseminated.

So, I think the hearings are important in another respect, namely to call attention to the fact that this is going on, and it's going to go on. We're going to use the computer.

We're going to use matching techniques. But we also have to be equally rigorous in our insistence that we be concerned about due process and about "unreasonable searches and seizures," not in a physical invasion, as such, into the household of the person, but an invasion into records, into the information that's disclosed to doctors, the information that's disclosed to banks, or whatever.

And if we fail to maintain that kind of sensitivity, then I suspect, in a very short period of time, we'll again fall down to that golden calf and talk about efficiency only.

That's the reason I'm suggesting—not to say we shouldn't have computer matching. I think we should. Not to say that we can deny the use of the computer—that would be foolhardy.

Mr. KUSSEROW. Mr. Chairman, I think a large part of your concern, as well as all of ours, can be met if we look at this thing by saying "What do these matching projects and different types of screens do?"

We know that there are certain things that we consider to be an inappropriate pieces of information in the file. Person's names should not be in the file if they don't have a proper social security card.

So, the problem we should be addressing is to make it clear what our effort has been on this project—what does not belong in there, if we could only move that to the front end and not permit erroneous data to get into the computer in the first place. Then you would remove a lot of the intrusiveness that goes with matching after the fact.

A case in point would be this. We would make an initial match of the death information and collect some monies. Then I would not let the medicare death information get back into the system. I would wait a couple of years, then do another run of my match data. I would come up with more millions of dollars and thousands of more people that are dead and still receiving checks.

However, I don't think that was the intent of the Congress when they created the Inspector's General Act and came up with all kinds of money to justify their existence. Rather, we were created to correct the system.

Now, if I can know what's wrong, I should correct that system. I should move to have a linkage so we could eliminate that problem so no one could get into the system and continue to receive benefits after they've died or no one could apply for a program benefit with an invalid social security number. If we can start doing that across the board, then I think we can have far fewer matches after the file has been developed, and it would be far less intrusive. And that is a lot of what we're trying to do here.

I'd also educate these people over to the front-end and not wait until they're already in the system—don't let them get in the system if they don't belong, or challenge them up front.

Senator COHEN. Mr. Kusserow, one final question before I yield to Senator Levin.

I mentioned before about certain programs that the President's Council had described in terms of their clearinghouse index. One was the program Sonoma, the so-called welfare queen.

I would like to know, No. 1, was that program ever performed—was that project every performed?

Tell me, how do you make up that profile? How would the profile of a "welfare queen" be made up?

Mr. KUSSEROW. First of all, I can give you, Mr. Chairman, for the record, a detailed analysis of what the program was all about.[1] But let me give you an example of how you might develop the profile. The trick in developing a profile is to have a high degree of probability that if you get a hit that in fact what you're looking for is what you're finding.

Let's say, for——

Senator COHEN. You're working backward. Start from the beginning.

If you get a hit, then you develop a good profile. I want to know how you develop the profile.

Mr. KUSSEROW. The point is we want to develop a profile so that whatever pops out will, in fact, be what you're looking for, not something else. Let me give you an example of elements that would go into developing the profile of a welfare queen. Suppose you have a situation where you have somebody who had 12 dependents, AFDC dependents. And let's say add to it the fact that none of these dependents—let's say they're all of school age, and none of them are enrolled in school. Let's say, also, that if they're on AFDC, the chances are——

Senator COHEN. How would you know that?

Mr. KUSSEROW. I'm just saying how to develop something that would turn into a profile—some elements that you could build into it.

Senator COHEN. So, you say, No. 1, a large number of children. Let me just continue with what you've said—a large number of children and, two, children not enrolled in school.

Mr. KUSSEROW. If those children are not enrolled in school, they aren't receiving any medical benefits under medicaid. You start adding things like that, somewhere along the line you'd have to raise a question, are there really children there? Are there real children? And are the benefits that are being derived from that process legitimate?

---

[1] See p. 407.

Senator **Cohen**. I want to go back to the beginning now and start with a group, AFDC.

And you say, "All right, we're going to see if we can find fraud or waste in that particular group. Therefore, in order to determine whether there is fraud or waste in that program, No. 1, we're going to be looking for the number of children that the mother has or the family has." Right? That would be one.

Before you set the profile up, you look for a number of children; right?

Mr. **Kusserow**. We may or may not.

Senator **Cohen**. But that's one factor you probably would look at. I'm just following what you said to me.

Mr. **Kusserow**. Let me back up, then, a little bit. The first starting point for a profile such as this would be what has been our experience of people that have been discovered being a "welfare queen," if you will. And we find that a large number are individuals that fabricate children—they really don't have the children that they claim—and therefore are able to get all kinds of extra AFDC benefits. So, you ask the question, in trying to build a profile, to surface those types of individuals. You might say, "Well, how could we find out whether, in fact, the children are nonexistent? How do you go about doing that?"

One of the things you might say is that if you have children, and you have a large number of children, it's fair to assume that children get sick. Certainly my child gets sick on a more regular basis than I care to have. And you'd say that if a person had this many children and has medicaid, then he or she should be billing medicaid for medical services for their children. Certainly if they have children of a school age, they should be enrolled in school.

So, you say if there was a large number of children and if they were not in school and if they were not receiving health benefits, what are the probabilities, therefore, that the children may, in fact, be nonexistent?

If you keep adding factors like that, based upon your experience from investigations, you could reach the point of saying that if you have enough identifiers hit like that, you'd have, say, a 90-percent probability that you'd have somebody who would be a "welfare queen" hitting the AFDC program.

You could then turn around and develop a program to surface all like characteristics with that degree of probability. That might be a way that you could go about developing a profile. For example, for a physician that might be defrauding medicare or medicaid, or that, let's say, a dentist—a dentist that performed 14 different types of drillings on a single patient. Fine, you may have had one patient that had a lot of bad teeth.

But if, after a while, you have a strong enough pattern develop, you could then design a program to say, "Give us a dentist that has an inordinate number of illnesses per client. Give us the worst examples. First, we'll start all the way down." Then, you test the data, and you may find that you have somebody, a dentist, that might be charging medicaid for dental services that are inappropriate, especially if you were to measure that history against a history of the patient and say that the patient did not have that many fillings in his or her mouth when he or she applied for certain other benefits. So, there are a lot of ways in which you could develop profiles.

Senator COHEN. Would you ever include race in developing a profile for welfare recipients? Would you take into account, say, black, white, yellow?

Mr. KUSSEROW. I wouldn't, offhand, do that unless there was pretty strong statistical evidence. And I'm not aware of any statistical evidence that would make that a significant factor.

Senator COHEN. What I'm asking is whether that could be done.

Mr. KUSSEROW. For most of the programs, you don't have any way in which to determine race.

Senator COHEN. In many of the applications, you've got to put down what your race is.

Mr. KUSSEROW. In many of the other programs, you're prohibited from asking.

Senator COHEN. The reason I raise that is because the Washington Post has been doing a series, for example, on what took place during the Second World War. They started gathering up people of Japanese descent.

If you now have the computer available to you and you have that information on file, such actions certainly could have been facilitated, couldn't they?

Mr. KUSSEROW. Before you are appropriately able to develop a screen or a profile for fraud or abuse, you'd have to have a strong demonstration that that was a relevant factor.

Senator COHEN. All I'm asking is what kind of protection do you have as to who is making these profiles? Who sees that information? How do we know what is in the profile of a "welfare queen"?

That's the reason I asked that. I just want to know what factors you look at. How do we know information is being compiled down there, or somewhere, so that we know what sort of activity big government eventually is looking at and accumulating information on? That's the reason for the question.

Mr. KUSSEROW. You have to go from historical experience. You start out—if the purpose is to identify people who are defrauding the program with any criminal acts, then you start off, like any researcher would—looking at people who have been convicted in the past and discovered in the past, looking at them for characteristics that would identify them. But then you'd always want to test it, test the hypothesis and test the assumptions, because you could have explanations for hits otherwise.

Senator COHEN. I have been told in another hearing that there was a greater probability of students coming from low-income families would default and not pay their student loans.

Now, is that a reasonable factor or an assumption?

Mr. KUSSEROW. I certainly couldn't see, unless you could demonstrate the relevance, why they would want to surface that information.

Senator COHEN. Yet, that information could be part of a profile if you're really trying to find out who defaults on student loans. You start looking at income levels of parents and then start focusing on those students coming from low-income parents, and therefore a higher probability, of a "raw hit."

Mr. KUSSEROW. But you'd never go off a single identifier.

Senator COHEN. I'm not talking about the single identifier. I'm talking about the tabulation of factors which may or may not be fair or even probable, but nonetheless somehow get put into that computer profile in which certain acts were taken.

I want to know who sees it, who knows?

Mr. MCBRIDE. May I comment a moment, Mr. Chairman, on the subject of profiling?

My background as a 20-year career prosecutor comes to the fore. Obviously, there are logical and deductive steps that one takes in terms of targeting anyone for investigation, whether it's an embezzler or a defrauder of the FECA program, or what have you.

I think Mr. Kusserow is correct. When you look at history, it's eminently a deductive process. You have 50 or 100 cases. You look at what kinds of people those were. And I don't think, in a logic sense, any attribute would be necessarily ruled out.

Senator COHEN. Would race be ruled out?

Mr. MCBRIDE. I don't think it need be, viewing the matter solely as a question of logic and probability. However, I personally would certainly never use race as a profile characteristic. But then, I have never come across a situation in which it has been probative, if you will, or relevant in terms of the population.

Senator COHEN. What if some statistician could say that there are more defaults on loans from low-income black families?

Mr. MCBRIDE. That's a sort of a "so what." You're not going to cut off their loan eligibility. And if they're delinquent, you're going to go after them whether they're black or white. So, why are you asking the question?

Senator COHEN. But you may develop a profile, taking race as a factor into account.

Mr. MCBRIDE. A profile for what?

I mean, you know your delinquent population. You know who hasn't paid their loan. You don't have to do a profile to find that out.

Senator COHEN. But if you're talking about matching, you don't always know who's working for the Federal Government, who hasn't paid their student loans.

Mr. MCBRIDE. Well, those matches are neutral.

We're at a university now, where we're, of course, concerned about policing the student loan program. Indeed, Stanford University has one of the lowest delinquency rates of any university in the country. But that's because we've aggressively pursued delinquent loans. We haven't looked at economic status, race, age, or any other factor. If you haven't paid, we go after you.

And I certainly think it would be grossly improper to try to do a statistical analysis of the delinquent population and then withhold eligibility for future loans from those who met the characteristics. I mean, that's the grossest kind of unfair stereotype.

Senator COHEN. I agree.

Mr. MCBRIDE. So I guess I'm puzzled by the relevance of this. If you're looking at a medical provider who gives every patient 400 stitches, you know, you've got a problem.

Senator **COHEN**. All I want to know is how much information is being collected on an individual; what sort of characteristics are being fed into the computer; what sort of characteristics are being taken into account by some bright, young computer programer who decides you can build a profile, taking into account the following characteristics.

I just want to know what the process is.

Mr. **MCBRIDE**. It's deductive. Let me make two other points: I mentioned FECA; there our investigative experience was that otherwise able-bodied men with lower back injuries was the basic parameter of the profile.

I think you could say it proved out. There's an awful lot of logical deducation in there, too. Obviously, somebody who is blinded at work and disabled is less likely to be clandestinely employed than somebody who has some arguably undiagnosable back injury.

The second thing is that profiling is somewhat like generating raw hits. Profiling doesn't determine anybody's benefits.

Senator **COHEN**. Raw hits terminated the benefits in Massachusetts.

Mr. **MCBRIDE**. Well, it shouldn't have.

Senator **COHEN**. I know that it shouldn't have but it has.

Mr. **MCBRIDE**. Well, you can't blame computer matching for misguided administrative judgments. People will do that with or without the computer.

Senator **COHEN**. Well, it's made a lot easier with the computer to simply take that raw information, suddenly terminate benefits in Massachusetts, and it's now in the courts.

Could someone argue that, first you may have violated due process; second, it may be an unreasonable search and seizure; and third, you may have invaded my privacy, based upon a computer determination that I had assets in the bank.

Mr. **MCBRIDE**. I agree, but if we're doing a profile of the union embezzler, let's say, who met all the characteristics, from hundreds of Labor Department investigations that we've done over the years; and then generated a list of 12 names, I cannot, based on that list, get 12 convictions for embezzlement.

That is a lead, and it's a rational, logical sorting of a potential population for investigation.

Mr. **KUSSEROW**. I think it needs to be emphasized that what you're doing with computer applications is reducing what you're looking at, and much of what we're trying to do is not trying to substitute one very labor-intensive activity—that of reviewing files manually for another labor-intensive activity which is generating huge volumes of data that then have to have somebody sit down and go through and follow up on.

You want to have a very restricted, limited quantity for someone to review, but it's only the first step. As a former prosecutor, you recognize that you want to see the intent element proved, you want to see all the other elements the statute demands before you even consider prosecution. So you're not going to take off a little printout sheet and say, well, somebody should be prosecuted or cut off from the program.

Making a decision either way to prosecute or to present you to a program official for cutting you off for a benefit based upon the computer printout without anybody actually putting human gray matter to that is a grave mistake and something that neither Tom or I would endorse, and we both deplore. We're trying to educate everybody else around to realize that it's not cost-effective to do things like that.

I'm sure if what you're saying about Massachusetts is true, that they're going to find there will be more labor-intensive activity trying to rectify what should have gone through a human process of reviewing files and discussing before taking any kind of action.

Mr. McBRIDE. I was going to say, in speaking of profiling, I would guess that the largest user of profiling techniques to sort out a large population for a followup verification and investigation is the Internal Revenue Service, and we all know that they have statistical screens on the amount of deduction, type of deduction, all sorts of things, and that that's the basic predicate of their targeting, their audit effort, I myself having been the victim of it 1 year when my deductions were way up—having gone through a painful audit, with the result of which I owed them no money—know the bother that that can cause, but still defend it as a logical means of targeting.

I think if we're concerned about the appropriateness of the profiling techniques within the Federal Establishment, (a) IRS is probably where there is more of it, and (b) more administrative action, or unnoticed administrative action, taken, based on it.

At least in the Massachusetts example it's immediately known and on the front pages, and lawsuits are filed. We have corrective measures to prevent that kind of thing from recurring.

Senator COHEN. Senator Levin, you've been most patient.

Senator LEVIN. Thank you, Mr. Chairman. Let me just pick up where Senator Cohen left off with some questions about profiles. First, I want to relate an experience which I had, that isn't directly connected with what we're talking about this morning but which raises some of the same questions.

Then we can work backward on some of the questions we're talking about this morning. I think I became most interested in the computer when I learned about credit card redlining, where a computer was used by the private sector to determine how quickly people in various States paid their bills.

It was determined that in certain regions, certain States, certain counties, certain metropolitan areas, certain groupings of ZIP codes, that the average payment on an oil company's bill was 30 days. For another batch of ZIP codes it was 40 days, another batch of ZIP codes, 24 days. And the computer is able to provide any kind of correlation you want. It can correlate age, for example, how quickly the people from 50 to 60 pay their bills, how quickly the people from 40 to 50 pay their bill. Anyway, I happen to live in a big city named Detroit, and Detroit was redlined by the credit card companies. We were given low points because our people, according to some computer, took 43 days to pay, whereas folks in southern Ohio only took 38 days to pay their bills. And when it came to scoring credit card applications, people from the city of Detroit were given lower scores, and frequently were told that they were rejected for credit cards because of their geographical location.

Needless to say, that created some problems. When I came to Congress I tried to correct it, so far with utterly no success.

Senator **Cohen**. Do you have a credit card?

Senator **Levin**. Mine's being taken away for other reasons. [Laughter.]

But I got very much interested in the correlations question. I don't doubt that you can prove that people who live in some ZIP code areas—now we have nine-digit ZIP codes—take 37 days, and the average person in some other ZIP code areas takes 39 days.

I don't doubt the accuracy of the computer; I doubt the relevance of it. I doubt the wisdom of treating individuals that way because of where they live. I think it's despicable and wrong in this society to judge folks because they happen to live in a ZIP code area where the average is such and such in terms of payment of bills.

I think we're going to dehumanize and deindividualize this society of ours, and that's really what got me interested in the use or the abuse of the computer, as far as Federal legislation is concerned.

Now, let's go back to what Senator Cohen was talking about—that question about profiles. Let's assume now that—I'm going to go back to something that Mr. McBride actually has experience with; that has to do with emergency loans to the FHA and disaster records of the SBA. You're not supposed to get both, I gather.

You match the two lists and find some folks who got both. Now you've got so many on that list that you couldn't prosecute all of them; you had to select. And this happens frequently for prosecutorial purposes: you've got the hits but sometimes there are so many hits you have to decide which hits you go to first. You determine by computer that there's a greater statistical likelihood that wheat farmers are going to cheat than dairy farmers—what a nice neutral subject I've picked here; I've stayed away from race and a lot of other things, although wheat farmers and dairy farmers will hate me, but other than that it will be all right.

Now, wheat farmers statistically are more likely to double loans than are dairy farmers. Wheat farmers are the more likely bad guys. Should we go after them first when looking at the hits because we know statistically there's a greater likelihood?

Mr. **McBride**. Well, first, if, as in the hypothetical you used, your data population is such that you can do the whole population, that's the best, and that's what we did.

Senator **Levin**. I understand. Now what we have to select is my assumption.

Mr. **McBride**. The computer selects.

Senator **Levin**. No, we have to pick from the computer list; I'm saying the list was 40,000 people who are in both lists. We can't go after all of them, so were doing some selection.

Mr. **McBride**. We're not at the point in the decision as to who we're going to prosecute, we're at the point of trying to find out who got two loans, and wheat or dairy is an irrelevance, we're coming up with a list of 200 people who could be an amalgam of wheat, dairy, cotton, soybean, and sorghum farmers; and they all got loans.

Then your logic exercise is in picking a target for prosecution—and that is a decision made more by the prosecutor than by the auditor.

Senator **Levin**. Well, the computer makes it possible for us to draw some statistical correlations. The same computer which pulled out those names is giving us some statistical likelihoods, and I'm asking the question: In your going after folks and your targeting folks—and now pursuing folks who have been selected by the computer—we know the correlations and the likelihoods—do you go after the most likely——

Mr. **McBride**. I have trouble dealing with the question. The profiling and sorting is something you do at the front end, that's something you do to massage the data and pull out, if you will, a fraud-prone population. You are not at that point in the decision at all as to who you're going to prosecute, because you have not done the followup verification and investigation to know who in fact committed the fraud.

That determination is very neutral as to the profile—you don't care what ages or what kind of farmer they are.

Senator **Levin**. Do you have any problem using the computer to tell us that there's a greater likelihood that that type of person—the person with 10 kids instead of 5 kids, the person who grows wheat instead of cattle—is more likely to have violated the law.

Mr. **McBride**. I have no problem with it, used to generate leads, if it has a logic-deductive base.

I have a problem with it, obviously, if it's used as a basis of prosecution, but I'm aware of no instance in which it has. I would be doubly opposed to it if it were used as a basis to determine future eligibility, and that gets to your credit card example, with its overtones of redlining.

Fortunately, the Federal programs and State programs are written so that people whose income levels are below a certain level are eligible, period. They are eligible.

The Federal Government cannot engage, thank God, in redlining, based on race, likelihood of fraud, sex, age, or any other improper factor.

Senator **Levin**. Mr. Kusserow, I'm wondering if you could comment on your testimony about student loans that are delinquent. You've indicated that some of the delinquent physicians were receiving hundreds of thousands of dollars in medicare and medicaid, and still owed the Federal Government money from student loans. You felt that was irregular.

I gather we are already taking some action on recovering these delinquent loans; is that correct? We're identifying those delinquents to see who's on the Federal payroll and then we're taking some kind of action, I presume, to deduct their loans from their wages.

Mr. **Kusserow**. We're talking about a very small student loan population, we're talking about the ones in our Department, as opposed to the Department of Education, but that was the first step. Once we found the match, we had to go behind and find what the reason for a hit was. We had to go back to the original loan files, to the circumstances surrounding it, go back to the individual and ask for an explanation. You go through a whole series of processes.

For example, for the people in our Department, we went through a whole series of steps for explanations, asking for reasons, and there are people that have reasons. And there are people that had explanations. For example, sometimes the school made a mistake on the records. We, therefore, corrected it and cleared the problem. Then you reach a population where they clearly have an ability to pay and they've made no attempt to go to the university and work out a repayment schedule. At that point then, the program managers make the decision as to what they feel they should do to encourage that individual to start paying back on their loans.

Senator LEVIN. What do you do to encourage that person?

Mr. KUSSEROW. For the employees in the Department—fortunately we're talking about a very nice population of people because physicians generally don't care to be called deadbeats in their community, so they're more than happy to take out of petty cash in most instances and pay off their loans.

In our Department all of a sudden the delinquencies evaporated among our physicians. For the people who participated in medicaid and medicare, similarly, their delinquencies are also evaporating by the fact that they're paying them back.

Senator LEVIN. Without now limiting it to your Department, we've got this long list of people who owe student loans—delinquencies. Do you have any problems with the IRS taking that list and seeing who it is that they're sending refunds to this year that owe the Government money on student loans—that kind of a match?

Do you have any problem with that match?

Mr. KUSSEROW. I would not entertain it in our Department at all.

Senator LEVIN. Do you have any objection on principle to a match between delinquent student loans and the IRS to see who they send refunds to, and then allowing the IRS to withhold that refund from anybody that owes the Government student loans?

Mr. KUSSEROW. There's a major question that would have to go in there, Senator, and that is, have you gone over that list of delinquents and have you determined why they're delinquent?

Senator LEVIN. The IRS would do that after they made the match.

Mr. KUSSEROW. No, sir, I would say that before you could get to that point you could consider making that decision. You would have to be sure that you've gone over the list of the delinquencies and determined what the reason for the delinquency is, and the fact that they've refused to pay back the money, and you have some reason to believe they have the financial capability of paying back the money.

Senator LEVIN. Would you do that before you make the match? You do that after you get the hit, don't you?

Mr. KUSSEROW. Yes; all the hit does is come up and say who's delinquent, in this case, who's delinquent that might work for our Department. But that's only the very first step because that's the machine effort.

Senator LEVIN. I understand. You object to the IRS taking that list of delinquents against their list of people that they owe refunds to, just to get a list of hits, and then going and talking to people and seeing do they really owe them money?

Mr. KUSSEROW. I thought you were saying to use that refund as a way of getting the money back.

Senator LEVIN. Of course. Once they get the hit they would want to see if the loan is really owed.

Do you have any objection to them obtaining the hits in the way I have described?

Mr. KUSSEROW. Yes.

Senator LEVIN. Even though after they get the hits they go and make sure the person really owes the money?

Mr. KUSSEROW. I think that is the step that should take place first.

Senator LEVIN. You didn't take it first; you did it after you got the hit.

Mr. KUSSEROW. That was the Department of Education, sir. That is not our Department. We don't operate at all that way.

Senator LEVIN. Is there anything in the regs or laws which would prohibit IRS from doing that?

Mr. KUSSEROW. Yes; but I defer to my colleague here for specifically——

Senator LEVIN. Is it prohibited by law?

Mr. MCBRIDE. My understanding is, yes, you can't offset against refunds. I don't know any purpose other than a tax collection purpose for which you can offset against refunds.

Senator LEVIN. Is there any reason why we should not authorize the IRS to set off against the refunds on these student loans once it ascertained they are really owed, just like these agencies?

Mr. MCBRIDE. I don't know. There is a certain logic. If the Government has given you some money, the Federal Government gave you a chunk of money for a loan, or whatever, and you owe it back, there is an irony when you owe Uncle Sam $5,000 to have Uncle Sam's other hand give you back another $5,000 as a tax refund.

But when you start translating it into particular programs—the medical loans, the student loans—that would be the direct Federal student loans, not the guaranteed loans which the banks make, if you get into that population; then if you start talking about social security overpayments, SSI disability overpayments, and then carry it a third step into the federally authorized and State-run program payments—like AFDC overpayments—you have a nightmarish welter of issues.

Closer to home, I know the former inspector general of one of the agencies, the VA, who felt very strongly that there should be an offset—these were direct government loans, thousands and thousands of dollars individually, millions cumulatively, and these people were getting big, big cash refunds—that there should be an offset against tax refunds.

Senator LEVIN. What is your conclusion on that issue?

Mr. MCBRIDE. I would be hesitant, because I can't see how you can distinguish one program like student loans from AFDC. And you would find the IRS system and voluntary compliance jeopardized by an attempt to offset billions of dollars and millions of transactions.

I would question it. But I do point out that there is a certain logic in saying, "Hey, Uncle Sam shouldn't be giving somebody $5,000. They owe Uncle Sam $5,000."

Senator **Levin**. It is the same logic, I presume, that Mr. Kusserow referred to when he said that it is irregular for a physician who is earning large amounts of money with the Government to be delinquent in his or her Federal loan.

I want to push this one step further. I want to keep the Federal student loan list. Now we have a number of people who got student loans that first year of school, dropped out of school, who haven't paid those loans back. That is the class I want to talk about, that particular group of delinquent loans. They don't register for the draft. A certain percentage of them have not registered for the draft.

The folks in Government say, "You know, the most egregious law violators are the ones that violate two of our laws: One, they haven't registered for the draft; the other one is they haven't paid back their student loan. We are going to go after the most egregious law violators first. We can't go after that half a million nonregistrants."

Mr. **McBride**. 585,000 is the last figure I saw.

Senator **Levin**. 585,000 sounds right. We can't go after all of them. Let's go after the ones that have done something else, in this case not paid back that student loan.

Any problem with matching those two lists and then deciding who to prosecute, based on egregious law behavior?

Mr. **Kusserow**. That would be a prosecutor's decision. I would say that prosecutor would have some problems if he was making a decision based upon something like that.

Senator **Levin**. The question is, from a moral point of view, do you see any problem matching those lists to help exercise that discretion?

Mr. **Kusserow**. I think there is a real problem with that, Senator. I think I would have the same concern that you have. That is, someone who has failed to pay back a loan, that is not a criminal violation. It might not be done fraudulently and to use that as a determination for who should be prosecuted for violation of some Selective Service Act I would have great problems with that, ethically, morally, and legally.

Senator **Levin**. Should there be any standards—let me ask Mr. McBride—on what they use these matches for? Should there be any kind of standards at all?

Mr. **McBride**. Well, yes.

Senator **Levin**. Do you know any standards as to the purpose?

Mr. **McBride**. There are presently no legislated standards. That is one reason I welcome the attention of this committee. I think the strongest case can be made for the application of matching where you are verifying eligibility for Federal financial benefits. I mean, that is where I think it is really appropriate; that is where the big bucks are.

If you start talking about matching, as has been proposed, and indeed may be done, tax data—particularly address information on the return—for purposes of enforcing a draft registration law, that, to me, presents a lot more problems. It is much more tangential. It is not a Federal financial benefit.

But that is up to Congress. If they want to mandate that kind of access, OK. They have mandated recently for debt collection purposes; for example, access to IRS address information, which may then be turned over, as I understand it, to private collection agencies. That at least is a Federal financial benefit, a delinquent debt owed the Federal Government. There is a little better nexus there.

But what I said earlier, you have to look. When you are talking about IRS, you have to look at what piece of data you want and what you want it for. And depending on that set, you are going to get a different answer every time.

Senator LEVIN. I take it you agree, Mr. McBride, that the matching is subject to abuse?

Mr. McBRIDE. Yes.

Senator LEVIN. Then we should devise some legislation to prevent abuse.

Mr. McBRIDE. I think you should devise legislation to prevent abuse and to encourage matching.

Senator LEVIN. To regulate matching?

Mr. McBRIDE. Yes.

Senator LEVIN. I agree with the chairman. Obviously, you want to use matching for legitimate purposes, and you want to make sure it is never used for illegitimate purposes.

We have got a monster here we had better control. I have seen it, at least in the private sector, go out of control. I am talking about credit card redlining. In that case, there were probably more correlations, but I think it amounts to the same thing. Use the computer, make correlations.

It is the use of technology to target certain groups which is socially vicious. We can do that in Government very, very easily.

Again, it is human nature we are talking about, not the computer. We should be devising statutes. There are potential abuses—we will say potential—there may be real ones right now in Government. There certainly are in the private sector.

I would ask, if the chairman agrees, that we should urge the witnesses to give us a specific list of the standards which we could adopt, what is proper and what isn't, in terms of matching.

You have dropped the requirement of cost-benefit analysis. One of the real restrictions on doing this is cost-benefit requirements. Economics tends to put some limitations on the mechanism. Otherwise, agencies could go wild. Good old economics will put some restraints on it.

We want to consider, I would think, whether we want to again require, as we once did, a cost-benefit analysis before doing a particular match. Could the witnesses give us, perhaps for the record, because I know we are running out of time, their suggestions on standards which should be applied as to whether a match should be allowed—considering such factors as a cost-benefit analysis—and again, as the chairman has indicated, the question of notice adequacy.

In order to cut short my questions, Mr. Chairman, I particularly would welcome from our witnesses the elements of the statute, the legislation.

Mr. McBride, particularly, in his last paragraph says that the Congress should urgently address the issue of needed legislation. To quote Mr. McBride, "It is urgent that Congress address the need for carefully drawn legislation to balance these privacy concerns against the need and the legitimacy to obtain data."

On the audit function, I have fewer problems. Beyond that we start getting into some very, very sticky areas.

We all know all the witnesses can give us specific suggestions for legislation that will hopefully carry out what the chairman has in mind in terms of these hearings.

Before I terminate my questions, I again want to commend Senator Cohen for initiating these hearings. I think we are really getting into some very critical areas. They are very difficult. You probably can't jump to conclusions, but, by God, we had better reach some before this technology absolutely consumes us—by invading our privacy, dehumanizing us, and deindividualizing us by making correlations on group bases which make no sense and which are unfair to individuals.

At the same time we must use this technology to help us go after waste and fraud and abuse, and I will tell you, there is plenty of it in Government. The public is losing its patience with it.

A lot of support for our programs has been eroded by fraud and abuse and waste. I think we will support those purposes if we can root them out by using the computer to help us root them out. I think we would be actually serving the purposes of some very noble programs.

It is that balance which you have all addressed yourselves to. Again, I just simply want to thank our witnesses for their presentation and thank the Chair for what he has done in raising these issues today.

Senator COHEN. Senator Levin, thank you very much for your participation in the hearings. As always, you bring acute analysis.

Mr. KUSSEROW. Mr. Chairman, I would just like to tell the Senator we would be more than happy on behalf of our department to supply the information that you desire.[1]

I would like to make one point, though. That is the fact that we are talking about a very small number of computer applications which are being done for auditing purposes.

I would point out, for example, our Department has 5,000 different computerized systems. In that Department there are probably tens of thousands of computer programs that are operating. So my concern—and I think Senator Levin's concern—should be focused in the area of programmatic decisions being based upon computer analysis, which is something that has absolutely nothing to do with what the Inspector General community said.

Congress specifically prohibited us by statute from being involved in making program decisions. So the larger question is not really looking at computer technology for audit purposes so much as it is in insuring what types of program decisions are being made on computer analysis in that larger arena, where 99.9 percent of the computer programs and computer applications are being applied on the program side.

Senator COHEN. Thank you, Mr. Kusserow and Mr. McBride.

---

[1] Information not available at time of printing.

Just a final question. In addition to what Senator Levin has requested, we may have a series of questions to submit to you, but I would like also to focus upon the oversight function as to who is overseeing all this.

Also, I would like to discuss the notice question which we talked about, because, Mr. McBride, you had a quote attributed to you early this week in the New York Times where you indicated that some computer matching programs have been established by certain Federal agencies in an incremental way. Perhaps you could elaborate on that as well.

Essentially, what Senator Levin and I have been suggesting here today—and we really do appreciate your testimony; you are two experts in the field—is that there is an ethical question involved.

What Senator Levin talked about as far as redlining on credit cards has also been true historically with mortgages. We have been through legislative battles on redlining by banks, based upon geographical locations, intercity areas, based upon those who live in those areas, and I would just submit to you race has been taken into account in many instances in the past, which is one reason why you have had congressional action barring redlining by banks for mortgage money purposes, the use of sex as a determinant, or race.

All of these social issues have come to the front because of practices by the private sector and, indeed, by the governmental sector.

What we have is an ethical question involved because computers don't deal with ethics. We have got to avoid the seduction of the sort of scientific ethic that whatever is possible is doable. We don't want to follow that "whatever is possible is doable" without having some sort of leavening effect at least by our ethical questions. We don't necessarily want to do that if we consider it to be inconsistent with our traditional notions of fairness, due process, of respect for individuals; and that is really the balance we are all striving for.

I think you have been very helpful, at least in discussing those terrible dilemmas that we face in the use of the computer in the future, but we look forward to receiving your written testimony as well.

Thank you for appearing.

Senator LEVIN. Mr. Chairman, as the old matchmaker would say, "There are matches and there are matches." [Laughter.]

[The prepared statements of Mr. Kusserow and Mr. McBride follow:]

THE PREPARED STATEMENT OF RICHARD P. KUSSEROW, INSPECTOR GENERAL, DEPARTMENT OF HEALTH AND HUMAN SERVICES

I AM RICHARD P. KUSSEROW, INSPECTOR GENERAL OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS). I WOULD LIKE TO THANK THE SUBCOMMITTEE FOR THE OPPORTUNITY TO DISCUSS OUR WORK ON COMPUTER MATCHING. THIS IS AN ACTIVITY "CHARGED" WITH MYTH AND MISUNDERSTANDING. MY COMMENTS TODAY ARE DESIGNED TO CLARIFY THE NATURE AND INTENT OF COMPUTER MATCHING AND TO ALLAY ANY ANXIETIES ABOUT NATIONALIZED DATA BANKS AND FEARS OF A "BIG BROTHER" SOCIETY. YOU HAVE INVITED ME AND MY COLLEAGUE, MR. THOMAS MCBRIDE, TO TESTIFY ON RECENT EFFORTS BY THE FEDERAL GOVERNMENT TO PROMOTE COMPUTER MATCHING AT BOTH THE FEDERAL AND STATE LEVELS OF GOVERNMENT. IN PARTICULAR, YOU REQUESTED THAT WE ADDRESS: (1) THE USE OF COMPUTER MATCHING TO PREVENT AND DETECT FRAUD, ABUSE, AND ERRONEOUS PAYMENTS IN GOVERNMENT PROGRAMS, (2) THE COST-EFFECTIVENESS OF COMPUTER MATCHING, AND (3) PUBLIC POLICY ISSUES RAISED BY MATCHING, SUCH AS PRIVACY RIGHTS OF INDIVIDUALS.

COMPUTER-MATCHING DEFINED

FIRST, I WOULD LIKE TO CLARIFY WHAT WE MEAN BY COMPUTER MATCHING. CHART I PROVIDES A LIST OF WORDS AND THEIR DEFINITIONS FOR YOU TO REFER TO. WE DON'T LIKE THE TERM COMPUTER MATCHING, WE MERELY USE IT AS A TERM OF CONVENIENCE. JUST AS WE PERFORM MANUAL AUDITS TO EXAMINE AND VERIFY DATA IN ACCOUNTS AND PROGRAMS, WE APPLY COMPUTERIZED PROGRAMS TO EXAMINE FILES TO VERIFY THE DATA, AND IDENTIFY THAT WHICH DOESN'T BELONG. COMPUTER MATCHING, THEREFORE, IS A TYPE OF COMPUTER AUDITING TECHNIQUE THAT INCLUDES SCREENING, EDITING, AND SCANNING BETWEEN LISTS, FILES, OR DATA WITHIN THE SAME LIST OR FILE - TO DETERMINE WHETHER IRREGULARITIES EXIST BETWEEN THE LISTS OR FILES. FOR EXAMPLE, WE HAVE COMPARED A LIST OF OVERDUE SCHOOL LOANS TO HEALTH PROFESSIONALS WITH A LIST OF DEPARTMENTAL EMPLOYEES AND MEDICAL PROFESSIONALS RECEIVING PAYMENTS FROM THE MEDICARE AND MEDICAID PROGRAMS. WHEN WE DID THIS MATCH, IT SHOWED THAT SOME PHYSICIANS EMPLOYED BY HHS WERE DELINQUENT IN THEIR LOAN PAYMENTS, AND THAT SOME OF THE DELINQUENT PHYSICIANS WHO WERE RECEIVING HUNDREDS AND THOUSANDS OF DOLLARS FROM MEDICARE AND MEDICAID SERVICES STILL OWED THE FEDERAL GOVERNMENT MONEY FROM THEIR STUDENT LOANS. NOW, CERTAINLY IT IS IRREGULAR FOR A PHYSICIAN EARNING LARGE AMOUNTS OF MONEY FROM THE GOVERNMENT TO BE DELINQUENT IN HIS OR HER FEDERALLY SUBSIDIZED MEDICAL SCHOOL LOAN.

WE HAVE ALSO MATCHED DEATH RECORDS IN THE MEDICARE PROGRAM WITH SOCIAL SECURITY BENEFICIARY NAMES TO SEE IF PAYMENTS ARE BEING ISSUED TO DECEASED PERSONS. DEAD PERSONS ARE NOT ENTITLED TO SOCIAL SECURITY PAYMENTS! FURTHER, WE HAVE SCREENED FOR NAMES OF PHYSICIANS WITHIN A PROGRAM FILE TO DETECT THOSE WHO DOUBLE BILL MEDICARE OR MEDICAID UNDER DIFFERENT PROVIDER NUMBERS. THE PURPOSE OF THESE TYPES OF DATA COMPARISONS IS TO IDENTIFY THE IRREGULARITIES IN A PARTICULAR DATA BASE. WE ARE REALLY LOOKING AT THE DATA BASE FOR INFORMATION WHICH DOESN'T BELONG.

ONCE IMPROPER INFORMATION IS IDENTIFIED, APPROPRIATE VERIFICATION AND INVESTIGATIVE EFFORTS CAN DETERMINE WHETHER POSSIBLE ERROR OR FRAUD EXIST. THE MATCH AND SUBSEQUENT VERIFICATIONS AND INVESTIGATIONS SERVE TO "PURIFY" THE DATA BASE, E.G., TO ELIMINATE INELIGIBLE PERSONS FROM FEDERAL PROGRAM BENEFICIARY LISTS. WE ARE THEN FREE TO PROTECT THE DATA BASE FROM BEING "POLLUTED" THROUGH "FRONT-END" EDITING TO VERIFY, FOR EXAMPLE, ELIGIBILITY FOR STUDENT LOANS, BENEFIT PROGRAMS, OR TO DETERMINE APPROPRIATE PAYMENT FOR MEDICAL OR OTHER SERVICES PROVIDED TO BENEFICIARIES.

AN EXAMPLE OF HOW THIS CAN WORK WAS A PROGRAM WE DEVISED TO DETECT NON-ISSUED SOCIAL SECURITY NUMBERS AMONG RECIPIENTS IN THE FOOD STAMP AND AID TO FAMILIES WITH DEPENDENT CHILDREN (AFDC) PROGRAMS IN ONE STATE. FROM A DATA BASE OF TWO MILLION RECIPIENTS WE ASKED FOR THE IDENTIFICATION OF ALL THOSE INDIVIDUALS WHO WERE USING A NON-EXISTENT NUMBER. WE CAME UP WITH 5,100 "HITS." ABOUT ONE-THIRD OF THESE WERE NUMBERS TRANSPOSED BY THE BENEFICIARY IN APPLYING FOR THE BENEFITS OR BY THE PROGRAM OFFICIAL WHEN "INSERTING" THE DATA INTO THE SYSTEM. THE REMAINING TWO-THIRDS WERE UNENTITLED OR FRAUDULENT. THE NEXT LOGICAL STEP WOULD BE TO MOVE THE DETECTION PROGRAM TO THE "FRONT-END" TO PREVENT AN INDIVIDUAL FROM PARTICIPATING IN A BENEFIT PROGRAM WITH A NON-EXISTENT NUMBER.

FRONT-END MATCHING--MATCHING WITH THE OBJECTIVE OF PREVENTING ERRONEOUS PAYMENTS--IS ALSO LESS INTRUSIVE AS ITS SOLE PURPOSE IS TO VERIFY ELIGIBILITY. FINALLY, FRONT-END MATCHING IS A PREVENTIVE MEASURE THAT RESULTS IN SAVINGS, MAKING MORE ASSISTANCE AVAILABLE TO PERSONS WHO ARE ELIGIBLE UNDER THE VARIOUS BENEFIT PROGRAMS.

THERE IS ALSO EVIDENCE THAT CLEANING UP A DATA BASE AND FRONT-END MATCHES HAVE A DETERRENT EFFECT. IN ONE STATE, FOR EXAMPLE, A NUMBER OF PERSONS ASKED THAT THEIR NAMES BE REMOVED FROM THE FOOD STAMP ROLLS, FOLLOWING A PUBLIC REPORT OF A MATCH OF PUBLIC ASSISTANCE LISTS WITH STATE EMPLOYMENT AND OTHER RECORDS. THESE PERSONS STATED THEY HAD FOUND WORK.

RIGHT TO PRIVACY

THE ISSUE OF PERSONS' RIGHT TO PRIVACY IMMEDIATELY SURFACES IN ANY DISCUSSION OF COMPUTER MATCHING. WE TREAT THIS ISSUE VERY SERIOUSLY AND HAVE WORKED HARD TO PROTECT PERSONAL PRIVACY. WE HAVE WORKED WITH OMB AS IT REVISED AND UPDATED GUIDELINES FOR COMPUTER MATCHING, AND DEVELOPED A REFERENCE PAPER TO HELP FEDERAL AND STATE GOVERNMENT AGENCIES IMPLEMENT THESE GUIDELINES. BOTH THE GUIDELINES AND REFERENCE PAPER ARE BASED UPON THE PRINCIPLES EMBODIED IN THE PRIVACY ACT OF 1974. THE GUIDELINES

PROVIDE FOR SAFEGUARDS OVER HOW INFORMATION IS TO BE USED, STORED, AND DISCLOSED. FURTHER, THERE MUST BE NOTICE TO THE CONGRESS, OMB, AND THE PUBLIC ON ANY MATCHING UNDERTAKEN BY AN AGENCY.

MR. MCBRIDE HAS BEEN INSTRUMENTAL IN THE REVISION OF THE OMB GUIDELINES ON MATCHING. GREAT CARE HAS BEEN TAKEN TO ASSURE THAT THEY PROTECT PERSONAL PRIVACY, AS HE WILL TESTIFY TO LATER THIS MORNING.

HISTORY

THOMAS MCBRIDE AND I BECAME THE CO-CHAIRMEN OF THE PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY (PCIE) LONG-TERM COMPUTER MATCH PROJECT AT ITS INCEPTION, IN THE SUMMER OF 1981. BEFORE I DISCUSS THE OBJECTIVES AND ACTIVITIES OF THE COMPUTER MATCH PROJECT, I WOULD LIKE TO PLACE THE CONCEPT OF MATCHING IN ITS HISTORICAL PERSPECTIVE.

MATCHING, PER SE, IS NOT A NEW CONCEPT. AUDITORS, INVESTIGATORS, AND STATISTICIANS HAVE BEEN MATCHING LISTS, FILES--DATA OF ALL SORTS--SINCE THEIR PROFESSIONS WERE BORN. IT IS A SIMPLE, THOUGH RIGOROUS, TASK NECESSARY TO ANALYSE DATA AND INFORMATION TO VERIFY THE ACCURACY OF THE DATA, DEVELOP CONCLUSIONS, OR TO ESTABISH POLICY.

As I stated earlier, using a computer to match data is a modern version of an old analytic technique. The advent of computer technology to store and retrieve masses of data has made it possible for us to develop computer techniques to scan, screen, and analyze that data.

We could sit down and manually look at two sets of data, for example, a list of persons receiving AFDC benefits and a list of persons for whom wages were reported in a given quarter. Manual review of the data would be costly in terms of the man-years of work required by the task. Using a computer, we can accomplish the same task more efficiently in several man-days. The computer provides us an updated auditing technique to establish common or related items in the compared information. From my perspective as Inspector General of the Department with the largest budget for Federal benefit programs, I must be concerned with using the best means available to audit our programs for purposes of preventing and detecting fraud, waste, and abuse consistent with existing laws.

Computer matching, as with generic matching, is not a new practice. We have researched, studied and continue to evaluate computer matching activities so that we can learn from them and build on best practices.

THE FIRST SIGNIFICANT COMPUTER MATCH OF BENEFIT PROGRAMS I WAS INVOLVED WITH WAS CONDUCTED IN 1976. THE FEDERAL BUREAU OF INVESTIGATION (FBI) MATCHED THE EMPLOYEE RECORDS OF VARIOUS GOVERNMENTAL EMPLOYEES AGAINST WELFARE RECORDS IN THE CHICAGO AREA. THE RESULTS OF THE MATCH WERE IMPRESSIVE: 4,600 "HITS"--INSTANCES OF GOVERNMENT EMPLOYEES RECEIVING BENEFITS IMPROPERLY--WERE RECORDED AND HUNDREDS OF FEDERAL AND STATE PROSECUTIONS FOLLOWED. SOON AFTER, THIS OFFICE, THEN A PART OF THE DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, INITIATED ITS OWN PROJECT MATCH WHICH COMPARED FEDERAL EMPLOYEE FILES AGAINST AFDC AND MEDICAID FILES. A PILOT CONDUCTED IN THE DISTRICT OF COLUMBIA ALONE IDENTIFIED OVER $330,000 IN INCORRECT PAYMENTS. BECAUSE OF ITS SUCCESS, "PROJECT MATCH" WAS EVENTUALLY CONDUCTED ON A NATIONAL SCALE IN 26 JURISDICTIONS.

MY OFFICE AT THE DEPARTMENT OF HEALTH AND HUMAN SERVICES HAS CONTINUED TO BUILD OUR RECORD OF COMPUTER MATCH APPLICATIONS. WE HAVE ENDEAVORED TO SHARE OUR EXPERTISE IN COMPUTER MATCHING WITH THOSE TASKED WITH SIMILAR RESPONSIBILITIES AT THE FEDERAL, STATE AND LOCAL LEVELS OF GOVERNMENT AND NOW WITH THE PRIVATE SECTOR.

WE HAVE PUT TOGETHER SEVERAL VOLUMES WHICH INVENTORY COMPUTER APPLICATIONS PREVIOUSLY OR PRESENTLY BEING UNDERTAKEN TO COMBAT FRAUD AND ABUSE IN OUR PROGRAMS. THIS COMPENDIUM WHICH COVERS

COMPUTER APPLICATIONS IN THE HEALTH PROVIDER, INCOME MAINTENANCE AND ASSISTANCE, AND FEDERAL AND STATE AREAS, REPRESENTS EFFICIENT AND ACCURATE MEANS TO REVIEW VOLUMINOUS AMOUNTS OF DATA. WITH YOUR PERMISSION, I WOULD LIKE TO HAVE THESE INCLUDED IN THE RECORD.

IN RECENT YEARS, CONGRESS HAS PASSED SEVERAL FEDERAL LAWS MANDATING MATCHING IN CERTAIN CIRCUMSTANCES. PUBLIC LAW 95-216, ENACTED IN 1977 AND EFFECTIVE IN OCTOBER 1979, REQUIRES STATE WELFARE AGENCIES TO USE WAGE INFORMATION CONTAINED IN STATE EMPLOYMENT SECURITY AGENCY FILES OR SOCIAL SECURITY FILES IN DETERMINING AFDC ELIGIBILITY AND PAYMENT AMOUNTS. LEGISLATION PASSED BY CONGRESS IN 1981 ALSO MANDATES WAGE MATCHING FOR THE FOOD STAMP PROGRAM. EFFECTIVE JANUARY 1983, STATE WELFARE AGENCIES MUST MATCH FOOD STAMP RECIPIENT FILES WITH WAGE INFORMATION FROM STATE EMPLOYMENT SECURITY AGENCY FILES OR SOCIAL SECURITY FILES.

THESE LEGISLATIVE INITIATIVES AND MATCHING OPPORTUNITIES WERE THE BACKDROP FOR THE LONG-TERM COMPUTER MATCHING PROJECT UNDER THE AEGIS OF THE PCIE.

LONG-TERM COMPUTER MATCHING PROJECT

ON MARCH 26, 1981, PRESIDENT REAGAN ESTABLISHED THE PCIE IN ORDER TO BETTER COORDINATE AND IMPLEMENT GOVERNMENT POLICIES

WITH RESPECT TO INTEGRITY AND EFFICIENCY IN FEDERAL PROGRAMS. THE PCIE IS CHAIRED BY THE DEPUTY DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET AND CONSISTS OF THE INSPECTORS GENERAL, AND REPRESENTATIVES OF MAJOR DEPARTMENTS WHICH DO NOT HAVE INSPECTORS GENERAL.

THE LONG-TERM COMPUTER MATCHING PROJECT IS CONSIDERED ONE OF THE MAJOR PROJECTS OF THE PCIE. ITS OVERALL OBJECTIVE IS TO EXPAND THE COST EFFECTIVE USE OF COMPUTER MATCHING AND RELATED TECHNIQUES TO PREVENT AND DETECT FRAUD, ABUSE AND ERRONEOUS PAYMENTS IN GOVERNMENT PROGRAMS USING EFFECTIVE SAFEGUARDS TO PROTECT THE RIGHTS AND PRIVACY OF INDIVIDUALS.

THE PROJECT FORMED FOUR WORKING GROUPS AND NUMEROUS SUBGROUPS TO PURSUE THE TASKS NECESSARY TO MEET ITS OBJECTIVES. THE WORKING GROUPS ARE:

1. MATCH OPPORTUNITIES
2. TECHNOLOGY AND PROGRAMMING
3. LEGAL AND ADMINISTRATIVE IMPEDIMENTS TO THE USE OF MATCHING
4. STATE/FEDERAL COOPERATION

CHART II LISTS THE MAJOR ACTIVITIES OF EACH OF THESE SUBGROUPS.

THE DEPARTMENT OF LABOR CHAIRS THE LEGAL AND ADMINISTRATIVE AND THE STATE/FEDERAL COOPERATION WORKING GROUPS, AND HHS CHAIRS THE OTHER GROUPS ON MATCH OPPORTUNITIES AND TECHNOLOGY AND PROGRAMMING. MY REMARKS ARE LIMITED TO THE ACTIVITIES FOR WHICH HHS IS RESPONSIBLE.

THE WORK GROUP ON MATCH OPPORTUNITIES WAS ESTABLISHED TO IDENTIFY AND ENCOURAGE MATCHING PROGRAMS AND TECHNIQUES THAT CAN PREVENT AND DETECT FRAUD, WASTE AND ABUSE IN GOVERNMENT PROGRAMS. THROUGH ITS WORK GROUP WHICH INCLUDES REPRESENTATIVES OF 4 STATES, THE DISTRICT OF COLUMBIA AND 22 FEDERAL AGENCIES, WE HAVE ACCOMPLISHED A NUMBER OF SIGNIFICANT TASKS. KEY AMONG THEM IS THE DEVELOPMENT AND DISSEMINATION OF COMPUTER MATCH PROGRAMS WHICH IDENTIFY IMPROPER SOCIAL SECURITY NUMBERS (SSNS) (SEE CHART III). KNOWN AS PROJECT CLEAN DATA, THE TWO COMPUTER PROGRAMS HAVE BEEN REQUESTED BY OVER 60 AGENCIES IN 40 STATES. HHS HAS ALSO SUPPLIED TECHNICAL ASSISTANCE IN USING THE PROGRAMS, AND IS NOW EVALUATING THEIR USE BY STATES.

A SECOND ACCOMPLISHMENT HAS BEEN OUR DEVELOPMENT, TESTING, AND USE OF A NUMBER OF PROGRAMS FOR NON-BENEFICIARY MATCHES. EXAMPLES OF THESE PROGRAMS ARE INCLUDED IN VOLUME III OF OUR COMPUTER APPLICATIONS VOLUMES.

THE WORKING GROUP ON TECHNOLOGY AND PROGRAMMING, COMPOSED OF REPRESENTATIVES FROM 5 STATES AND 22 FEDERAL AGENCIES WAS ESTABLISHED TO DEVELOP STANDARD PROGRAM DATA ELEMENTS AND EXTRACTION FORMATS, AND FRONT-END EDITING TECHNIQUES.

THE SUB-GROUP ON STANDARDIZATION OF DATA ELEMENTS HAS DEVELOPED A DRAFT SET OF COMPATABLE DATA ELEMENTS AND EXTRACTION FORMATS TO FACILITATE MATCHES BETWEEN BENEFIT PROGRAMS AT THE FEDERAL, STATE, AND LOCAL LEVEL. THESE DRAFT DATA ELEMENTS HAVE BEEN REVIEWED BY THE STATES AND A DRAFT FINAL DOCUMENT WILL BE READY BY THE END OF THE MONTH.

ONE OF THE MOST IMPORTANT ACCOMPLISHMENTS OF THIS WORK GROUP IS THE DEVELOPMENT OF AN INVENTORY OF STATE COMPUTER MATCHING SOFTWARE PACKAGES. THE INVENTORY IDENTIFIES, AS OF OCTOBER 1982, COMPUTER MATCHING CONDUCTED BY STATES WITH THE LABOR AGENCIES, THE SOCIAL SECURITY ADMINISTRATION AND OTHER PUBLIC AND PRIVATE AGENCIES. IN ADDITION, THE INVENTORY IDENTIFIES ON A STATE-BY-STATE BASIS FRONT-END MATCHING TO VERIFY ELIGIBILITY, INTERJURISDICTIONAL MATCHES WITHIN STATES.

COST OF MATCHING

BEFORE I SUMMARIZE MY COMMENTS, I WANT TO SAY A FEW WORDS ABOUT THE COSTS AND SAVINGS ASSOCIATED WITH COMPUTER MATCHING. WE

WISH WE COULD GIVE YOU HARD FIGURES ON THE COST-BENEFITS OF MATCHING. THAT IS NOT POSSIBLE AT THIS TIME FOR THESE REASONS: STATE AND FEDERAL AGENCIES HAVE GENERALLY INCLUDED THE COSTS OF MATCHING IN TOTAL DATA PROCESSING COSTS RATHER THAN BREAKING THEM OUT; AND THE FOLLOW-UP ON HITS ASSOCIATED WITH MANY MATCHES HAS NOT BEEN COMPLETED. THEREFORE, WE DO NOT KNOW THE EXTENT OF RECOVERY AS A RESULT OF THE MATCHES. WE ARE COGNIZANT OF THE NEED FOR DOCUMENTING THE COST-BENEFIT OF OUR ACTIVITIES AND WILL ADDRESS SUCH IN OUR CONTINUING EVALUATION OF MATCHING ACTIVITIES.

WE ARE CONVINCED, HOWEVER, THAT MATCHES RECOVER MORE MONEY THAN THEY COST. FOR EXAMPLE, NEW YORK STATE HAS BEEN MATCHING WELFARE RECIPIENT RECORDS WITH QUARTERLY WAGE REPORTS FROM NEW YORK EMPLOYERS FOR SEVERAL YEARS. THEY ESTIMATE THAT THEY WILL SAVE $114 MILLION FROM 1979-1983 FROM THE SYSTEM COST OF $28.1 MILLION. THIS IS A 4 TO 1 RETURN ON THE DOLLAR. IN 1981, CALIFORNIA MATCHES STATE INCOME TAX REFUND RECORDS WITH FILES ON RECIPIENTS ORDERED BY THE COURT TO REPAY OVERPAYMENTS FROM THE AFDC PROGRAM. THE COST WAS $6,000 FOR A RECOVERY OF OVER $200,000. OUR OWN PROJECT SPECTRE WHICH MATCHES SOCIAL SECURITY BENEFICIARY PAYMENTS WITH MEDICARE DEATH FILES HAS LED TO $7,525,957 IN RECOVERIES TO DATE. RECOVERIES, IN THIS CASE, COVERS ALL MONIES COLLECTED BY OUR INVESTIGATORS INCLUDING CHECKS NOT CASHED BUT DEBITED TO THE TREASURY. WE PROJECT TOTAL SAVINGS OVER TIME TO REACH $25.2 MILLION. (SEE CHART IV)

THESE ARE JUST A FEW EXAMPLES OF THE POTENTIAL SAVINGS FROM MATCHING.

CONCLUSION

I WANT TO CONCLUDE MY TESTIMONY BY STRESSING THE POSITIVE ASPECTS OF COMPUTER MATCHING. MATCHING IS A COMPUTER AUDITING TECHNIQUE USED TO VERIFY INFORMATION IN A LIST OR DATA FILE. WE MATCH TO "PURIFY" OUR DATA BASE SO THAT, FOR EXAMPLE, DEAD PEOPLE DON'T RECEIVE CHECKS AND BAD DATA DOESN'T LEAD TO POOR SERVICES. THEREFORE BY PURIFYING OUR DATA BASE WE HAVE MONEY AVAILABLE FOR SERVICES TO THOSE WHO ARE ELIGIBLE FOR GOVERNMENT BENEFIT PROGRAMS. I AM CONVINCED THAT MATCHING IS A COST-EFFECTIVE TOOL FOR ENSURING THE INTEGRITY OF FEDERAL PROGRAMS.

I HOPE MY COMMENTS ON COMPUTER MATCHING HAVE BEEN HELPFUL. I THANK YOU FOR THE OPPORTUNITY TO MAKE THIS PRESENTATION AND I AM AVAILABLE TO ANSWER ANY QUESTIONS YOU MAY HAVE.

Statement of
Thomas F. McBride
Associate Dean, Stanford Law School
(Former Inspector General of the
U.S. Department of Labor)
Before
Subcommittee on
Oversight of Government Management
Committee on Governmental Affairs
United States Senate
December 15, 1982

Mr. Chairman, I wish to thank the Subcommittee for the opportunity to testify on computer matching.

The Long Term Computer Matching Project, sponsored by the President's Council on Integrity and Efficiency, was established to promote the use of computer matching and related applications of modern information technology to help prevent and detect fraud and overpayments in government programs. That fraud and overpayments exist and amount to billions of dollars in losses to the Government every year is beyond dispute. The General Accounting Office estimated overpayments from five major benefit programs amounted to $867 million in FY 1979--$639 million in Federal funds and $228 million in State funds. 1/ By 1982, they estimated that, without corrective action, Federal

---

1/ "Legislative and Administrative Changes to Improve Verification of Welfare Recipients' Income and Assets Could Save Hundreds of Millions", January 14, 1982, General Accounting Office.

expenditures, because of overpayments in these five programs would exceed $1 billion. It is also apparent that the public increasingly has gained the perception that cheaters are successfully exploiting the nation's taxpayers and that management countermeasures have been insufficiently effective. This undermines not only support for the continuation of government programs, but also respect for the government itself. These are among the reasons the project was adopted and got underway.

There are 58 government benefit programs in which eligibility for participation depends on financial need as determined by an applicant's income and assets. In fiscal year 1980, Federal and State expenditures for these programs amounted to $102.6 billion. In addition, there are the large insurance and entitlement programs, such as Social Security and Unemployment Compensation, for which participation depends on such status factors as an individual's age, employment, and prior payments into insurance type funds. Social Security retirement benefits will probably cost some $150 billion this year and it is estimated that State/Federal costs for unemployment compensation may total some $26 billion for FY 1982. There are also other tremendous government expenditures involving such matters as highway construction, public works and defense contracting. Audits and investigations have amply demonstrated that fraud and waste occur in all of them and that modern computer applications can be employed effectively to help contain costs, prevent fraud, and detect overpayments.

At the outset, however, before discussing the organization and activities of the Project, there is one matter that I wish to address concerning, particularly, the use of computer matching as a tool to prevent fraud and overpayment in benefit and entitlement programs--programs that affect millions of Americans. That is the apprehension that computer matching may lead to possible invasions of privacy and violations of individual rights. Questions involving rights and privacy have been of concern to the Computer Matching Project from the beginning. In fact, the work plan for the project's operational phase characterizes the project's overarching purpose as expanding the use of computer matching and related techniques "with effective safeguards to protect the rights and privacy of individuals."

What we are talking about is, in effect, drawing a balance. On the one hand, government managers must responsibly employ the most modern and effective means available to ensure that the taxpayers' money is not being wasted through fraud and error. On the other hand, safeguards must be maintained to make certain that privacy rights are protected.

We believe that as far as Federal departments and agencies are concerned, the necessary safeguards to prevent abuses of modern computer technology that could violate individual rights or invade privacy are in place and are in compliance with the Federal Privacy Act of 1974 and the Office of Management and Budget Guidelines for Conducting Computer Matching Programs that are based on it. According to procedures, which have been laid down, one of the salient privacy concerns often expressed--that computer matching will incrementally lead to the development of a national data base containing complete information on everyone, that can be freely accessed and used--is patently impossible.

The Guidelines specify that as soon as a match is performed, the file that was used must be returned to the agency that supplied it or must be destroyed. Lists of the matching items or hits have to be destroyed as soon as investigations have been conducted. Thus, no files accumulate. In addition, there must be administrative, technical, and physical security safeguards for all files being matched in order to prevent unauthorized access. Files cannot be duplicated or disseminated within or outside the agency performing the match. They can be used or accessed only to match the files previously described and agreed to in writing. They cannot be used to extract general information, concerning individuals, that has nothing to do with the match being performed. Thus, fishing expeditions are precluded. These safeguards, along with

Congressional oversight and alert public interest groups, prevent misuse and abuse that could potentially result in harm to individual rights and privacy.

To put concerns about privacy and individual rights in further perspective, how computer matching actually occurs should be understood. If a person is examining records to discover possible similarities, duplications, contradictions or other related material, clearly he or she would have to scan or search through the files. A computer programmed to do a match, however, simply picks out and prints only specific items that match. Nothing else emerges from the machine. In this respect, computers are much less intrusive with regard to individual privacy than are people. It should also be recalled, that computers do not make decisions that might violate someone's rights or terminate entitlements. What the computer does is provide a list of apparently common or related items. It does no more than supply possible leads for investigation, follow up and verification. Computers do not and cannot automatically establish that fraud exists. They do not cut off benefits or payments mechanically.

Genesis of the Project

History

The first large scale use of computer matching in the Federal sector was HEW's Project Match in 1977. Matching

Federal military and civilian employee records with information from several states on recipients of AFDC, the project was an outgrowth of matches of welfare recipient and wage data that were going on at the State level. The match found 3,071 individuals who had been overpaid. Another 2,168 people were identified who were ineligible to receive benefits.

I was Inspector General at the Department of Agriculture at the time. Seeing the results of Project Match, I began to look at my own department to see where these techniques could be applied. Paying over $5 billion in benefits in 1978--and now over $10 billion in benefits--with recipient income the primary basis for benefit eligibility, the Food Stamp Program was the obvious choice.

We decided to pursue matching on a smaller scale than HHS by concentrating on specific geographic areas, minimizing the problems of gathering data from all over the country. We also decided to rely on the wage data gathered by the unemployment insurance program. In many states, wage data is collected quarterly for use in administering the unemployment insurance program. The information is from 3 to 6 months old, compared to Social Security's wage data that is 18-24 months old. It was decided to compare the "hits" with other income-based programs to see if overpayments had also occurred in them.

Mississippi was the first place this technique was applied; 763 overpayment cases were identified with over $760,000 in losses identified from Food Stamps, Medicaid, and Aid to Families with Dependent Children (AFDC). Using the same technique in Birmingham, Alabama, over 1,000 cases were identified with losses amounting to over $1 million to the Food Stamp Program; 748 cases were still participating at the time of the match. Their benefits were reduced or terminated with monthly savings amounting to $88,158.

In Memphis and Nashville, Tennessee, over 1,600 cases of underreporting of income in the Food Stamp Program were found through computer matching. Of these cases, 667 were also participating in the AFDC program, 735 in the Medicaid program, 95 were receiving Supplemental Security Income, and 144 were receiving housing assistance. The losses from these programs for the verified cases were over $3.0 million. Monthly savings for the Food Stamp Program were over $80,000; more than 1,200 cases had benefits terminated or reduced. There have been over 400 indictments to date. It was estimated that there was a $1 return for every 5 cents spent on this matching project.

In a recent match in the Atlanta area, over 3,000 cases of suspected food stamp fraud were identified. Overissuances from the food stamp program for these cases were expected to amount to over $3 million. Over half of the cases also were receiving AFDC, Medicaid, or housing benefits. More than 2,000 cases were still participating in the Food Stamp Program. The monthly savings from benefit reduction or termination amounted to almost a quarter of a million dollars.

Food Stamps was not the only program in which matching was used. The techniques are valuable not only in welfare programs, but also in other programs. In 1978, we matched emergency loans of the Farmers' Home Administration during 1977 with disaster loan records of the Small Business Administration. We found 123 excess duplicate loans amounting to $2,300,000. By the end of 1981, over $1.25 million had been recovered. The match cost $50,000.

Computer matching had proved itself to be a valuable technique for the detection of fraud and waste.

It was about this time that I became Inspector General for the Department of Labor where matching had been done for some time at the state level. Unemployment insurance benefits have been regularly compared with wage information to verify eligibility for unemployment benefits since the early 1970's. There are 41 states that collect wage data quarterly either by the state-administered unemployment insurance program or the state tax department, and Minnesota will begin collecting this information in 1984.

Matching has proven to be the most effective tool the unemployment insurance program has for detection of fraud. In 1981, California uncovered $18 million paid to individuals fraudulently claiming unemployment benefits. Kansas is able to recover $750,000 annually as a result of this type of eligibility match and another $1.2 million is saved by offsetting benefits. New Jersey, which just set up a Wage Reporting System, was able to identify over $3 million in overpayments by the middle of 1982.

The wage records maintained primarily by the state employment security agencies currently are the most valuable source of income information for many matching programs. In a survey conducted by the Long Term Computer Matching Project, 34 State labor agencies reported providing state social service agencies with automated wage information. This data is compared with information on recipients of AFDC, general state assistance, Food Stamps, and Medicaid, as well as other social service programs. In Illinois, the comparison with the AFDC files has yielded over $12 million in monthly grant dollar savings since 1975. Expected savings in New York from wage matching, including the unemployment insurance program, is over $114 million from 1979 to 1983. Costs for the Wage Reporting System and the matching program were expected to be $28 million over the same time period. This included development costs of the system.

These results, along with the need to demonstrate vigorous action to protect the integrity of benefit programs, were the impetus for the Long Term Computer Matching Project of the President's Council on Integrity and Efficiency.

The use of matching in the Departments of Agriculture, Labor, Veteran's Administration and other Federal agencies had shown it could be a cost effective tool for the detection and prevention of fraud and waste in benefit programs by providing an easy method to verify eligibility for benefits. Where cost information was developed, it had a high benefit to cost ratio. In other cases, where no cost information for the match was developed, the cost avoidance from benefit outlays was significant. As more and more programs move to checking wage and other eligibility information before making a decision on benefits--similar to what is done by banking institutions before granting a loan or credit--more costs will be avoided earlier in the benefit determination process.

It was becoming more and more apparent that computer matching was a quick, efficient, and highly effective means of detecting fraud and overpayments. In addition, the privacy concerns voiced by many at the onset of Project Match did not materialize. The present Administration sought to encourage the use of these techniques as an effective means to ferret out waste, fraud and abuse from federal benefit programs.

The Project

Approved by the President's Council on Integrity and Efficiency in September 1981, the Long Term Computer Project, chaired by the Inspectors General of HHS and Labor, sought to encourage and facilitate computer matching. The Project does not run computer matches. The project works on gathering and sharing information on computer matching and removing obstacles to the use of these techniques. This course was decided upon in light of our survey regarding the use of computer matching and the problems that were perceived by Federal and State agencies. It was clear that little information flowed concerning the use of matching, technology and the results among Federal agencies, among the States, and between State and Federal levels. It was also reported that the wider use of matching was inhibited by a broad array of legal, administrative, technical and coordination difficulties.

To accomplish this work of gathering and sharing information and removing obstacles effectively, the Inspectors General brought Federal and State program administrators into the project early. If computer matching is to be truly effective, it must be built into the actual administration of a program. Fifteen states and the District of Columbia, with a total of 26 representatives, sit on the project's four working groups There are 65 Federal representatives.

The project began by first surveying Federal agencies to see what they had done in computer matching. We then inventoried state matching activity. A great deal was going on. We needed to make this information widely available to program administrators, not just to those directly working on the project.

The project publishes a quarterly newsletter on computer activities. The newsletter highlights significant Federal and State matches and related activities, unique techniques and approaches and problems that should be considered in conducting a match. It goes to over 800 Federal and State agencies and officials, and to interested citizens as well.

Through the Federal and State representatives, an extensive network of contacts for computer matching and related activities has been built and is still growing. It is through this network and the newsletter, that the project has been able to serve as a broker. People interested in doing a particular type of match are put in contact with others who have done it before. If someone has encountered a problem in doing a match, ideas for resolving it can often be found through the network. By simply putting people in contact with each other, ideas for matching projects and ways to perform matches more efficiently are generated. This is the way the Project has encouraged the use of matching techniques.

The project also sought to address the numerous obstacles and difficulties blocking greater computer matching activities through four working groups, composed of the Federal and State representatives. The groups were organized around major issue areas--legal and administrative issues, State/Federal cooperation, technology and programming and match opportunities. The Inspector General of the Department of Labor leads the Working Groups on Legal and Administrative Problems and State/Federal Cooperation, and the Inspector General of the Department of Health and Human Services leads the working groups on Technology and Programming and Match Opportunities. Each group has identified major problems and developed recommendations for resolution of these problems. This work is continuing.

The Legal and Administrative Working Group has been looking at the OMB Guidelines for Conducting Computer Matching Programs, access to tax information, use of the social security number, quarterly wage reporting, state privacy legislation, and interjurisdictional matching. The Technology and Programming Group has completed an inventory of state computer matching software packages and also has been studying front-end editing techniques and standardization of data elements for matching projects. The Working Group on Match Opportunities has been looking at match-related techniques as they apply to fraud prevention, payment processes, and non-benefit programs. The Group also has made various software packages available to State and Federal agencies. Finally, the Working Group on State/Federal Cooperation has been acting as a project steering committee and has undertaken several studies.

State/Federal Cooperation

The Working Group on State/Federal Cooperation operated under my chairmanship. It consists of 9 senior State Government officials and 17 Federal agency representatives. It serves as an information and coordination channel to the States and as an overall steering group for the project, identifying salient problems to address, establishing work priorities and evaluating the products of other project working groups.

The State/Federal Cooperation Working Group is also dealing with several cross cutting issues that affect all the States. One task group is analyzing the major incentives and disincentives which exist for States to engage in computer matching, with the aim of developing recommendations for improvements. Another will examine problems involved in interjurisdictional matching efforts, particularly legislative, technical and coordinative impediments that make joint efforts more difficult.

Legal and Administrative Activities

Another project effort I chaired was the Legal and Administrative Working Group that addressed the major obstacles in this area that have tended to impede the use of computer matching by Federal agencies and the states. The Group is identifying and analyzing these problems with the purpose of developing recommendations, and, where possible, to solve them. The following are the major concerns on which we have been concentrating. Five states and 17 Federal agency representatives participate.

(a) Office of Management and Budget Guidelines for Conducting Computer Matching Programs: A team drawn from the working group of the project participated with OMB in an effort to revise the Guidelines in light of several years of operational experience with them. A revised version was published by OMB and went into effect on May 11, 1982. The new Guidelines are considerably simplified and are more practicable. They focus strongly on privacy, reflecting our commitment to maintain all the statutory requirements laid down in the Privacy Act of 1974. They provide for requirements that the use of data be compatible with the purposes for which they were collected and that routine use notices are published in the Federal Register to disclose how data will be employed. They also go beyond the Act's basic requirements in several significant provisions. For example, the new Guidelines provide for public notice that matching is being conducted to keep the public informed about matching activities by agencies. They also call for specification of information regarding the plans and purposes of matches and written statements regarding the use, safeguarding and disposition of files involved in matching efforts. These new Guidelines derive from our insistence that the rights and privacy of individuals must be protected, that matching must take place openly with full public knowledge and that records and documentation concerning matching activities must be maintained. The group also has developed a reference paper to assist managers in the implementation of the Guidelines with suggestions, procedures, cost-benefit analysis, and recordkeeping.

(b) Social Security Numbers: Clearly, the social security number has emerged _de facto_ as the closest thing to a personal identifier in the United States. It is currently employed by all levels of government and by the private sector for identification purposes. For computer matching, its wide use has proved to be invaluable, greatly simplifying the task of discovering relationships and contrasts among data items. Nevertheless, there are still areas in which social security numbers are not employed as identifiers; and the Social Security Administration still actively opposes its wider use and supports restrictions whenever possible, using arguments ranging from privacy to its own workload problems. I believe this is unrealistic and short sighted. A project subgroup has been exploring legal and administrative aspects of the use of social security numbers with the objective of considering recommendations regarding conditions and procedures under which its greater application might be arranged.

(c) Quarterly Wage Data: Millions of people participate in the 58 needs-based Federal benefit programs, such as Food Stamps and AFDC on the basis of their financial status. To be eligible, their income and assets must be below the amounts specified in program legislation. According to Quality Control data available for the Food Stamp and AFDC programs and studies by the General Accounting Office, the principal reason for overpayments in the needs-based programs appears to be underreported or unreported wages on the part of program beneficiaries.

The key data base for verification of recipient eligibility for benefits in needs-based programs is quarterly wage reports that employers make to states on individuals for the purposes of the unemployment insurance program. Quarterly wage reporting systems for unemployment insurance are currently operating in 38 states. Another three States (New York, Massachusetts and New Jersey) have instituted their own quarterly wage reporting requirements for the management of welfare programs. Minnesota recently adopted quarterly wage reporting for unemployment insurance by act of its legislature, to become effective April 1, 1984. Eight States, however, including Ohio, Michigan and Wisconsin, do not have this invaluable data base available and have no plans to establish it. In these States, the eligibility of recipients for program benefits is more difficult to verify.

The Computer Matching Project strongly supports draft legislation recently submitted to the Office of Management and Budget by the U.S. Department of Labor to mandate the establishment of quarterly wage reporting systems for unemployment insurance in all States. Studies by the Department of Labor and by the former National Commission on Unemployment Compensation proved that savings in administrative costs and overpayments in the unemployment insurance program alone in the 12 States not having quarterly reporting for unemployment insurance would pay back the entire cost of installation of the systems in less than two years.

This does not in any way take into account the incalculable potential savings possible in the needs-based programs through eligibility verification by use of wage data. If the State to have instituted a quarterly wage reporting system most recently, New Jersey, is a fair indication, such savings could be very substantial. In a report to the Governor dated April 1, 1982, total savings resulting from the first year of operation of the quarterly wage reporting system were estimated at $33.2 million at a cost of $4,917,040. We are convinced that the conduct of quarterly wage reporting by all the States would be a major step in countering fraud and overpayments.

(d) Access to Tax Information: Access by program managers to certain categories of tax information for anti-fraud purposes would also contribute greatly to efforts to verify eligibility for needs-based benefit programs and reduce fraud and overpayments. The Tax Reform Act of 1976 and IRS interpretation of it have served to make virtually all categories of tax information unavailable for verification and anti-fraud efforts. When access to tax data is suggested, concern is frequently expressed that IRS data includes a wealth of information about everyone in the United States and that it would be inappropriate and undesirable for such information to circulate freely throughout government. We strongly concur, and we are not advocating access to charitable, medical or other deductions or payments. A valid distinction can be made between information supplied by the individual taxpayer and financial information provided by such third parties as employers, banks, insurance companies and stock brokers. We believe that information concerning income and assets regularly and properly reported to IRS by third parties should be available to verify that individuals who seek assistance are eligible to receive it.

There is now adequate evidence that great savings would result if third party information on assets and income were available and used to ensure program integrity. The results recently reported of the initiative of Massachusetts authorities in using data available from state banks and financial institutions under provisions of state law clearly indicates this. On the basis of experience thus far, Massachusetts officially estimates that savings in the range of $136 to $306 million will be made in the State in the AFDC program alone and projects savings nationwide that could reach as much as $8.8 billion. Availability of other categories of third party information in possession of IRS would undoubtedly increase savings and curtail overpayments to a much greater extent.

Failure to employ information that is available deprives us of basic and necessary safeguards against deliberate fraud. In our estimation, there is no good reason why taxpayers--those whose tax payments make humanitarian government programs possible--should be held to higher standards by the government than people who benefit from such payments. Taxpayers are well aware that their tax returns and information submitted by third parties on their behalf are subject to computer matching to make certain that they are complying with the tax laws. Why should beneficiaries of needs-based programs not be subject to the same sort of safeguards to ensure that they are complying with the laws that specify conditions of eligibility for participation in such programs?

The argument is often made, however, that any lessening of confidentiality whatsoever regarding tax information would be dangerous because tax collections depend on voluntary compliance by taxpayers, which in turn depends on complete confidentiality. This argument does not withstand close scrutiny. First of all, it must be recalled that the information we have in mind is not taxpayer supplied data but reports submitted by third parties. It is hard to see how gaining access to third party data could adversely affect taxpayer compliance. Moreover, as Senator Nunn pointed out in a statement before the Subcommittee on Oversight of the House Ways and Means Committee on December 14, 1981, "Statistics compiled by both the IRS and the General Accounting Office indicate that voluntary compliance with the tax laws actually has decreased since passage of the Tax Reform Act of 1976... The GAO findings also refute the contention that voluntary compliance is in direct proportion to the degree of confidentiality of tax return information."

If Congress has seen fit to amend the Tax Reform Act to permit release of taxpayer-supplied information to assist in collection of debts owing to the government and to permit locating absent parents for child support purposes without undermining compliance, the third-party supplied information should be made available to verify eligibility for benefit programs to save the large sums that are lost through fraud.

It should also be pointed out that use of tax information to prevent or detect fraud and overpayments does not necessarily mean that agencies other than IRS would gain access to information concerning taxpayers. IRS could well maintain its sole control over tax information, if IRS itself would conduct matches of program recipient rolls with information in its possession. Technically running such tapes on computers is a very simple operation and IRS could easily do so. In such a case, only items that matched would be released with all the current safeguards that apply to matching activities in place. The basic confidentiality of taxpayer information would then be maintained and fraud control efforts would be greatly facilitated.

Summary

A basic issue running through the legal and administrative considerations I have raised is that of balancing the competing interests of privacy and individual rights on the one hand, and the legitimate government interests of eligibility verification and program integrity on the other. We must be sure that benefits are going to the right people, to those who are fully eligible to receive them. But we must also be alert and sensitive to the possible dangers of going too far, making sure that an appropriate balance with privacy concerns is struck. Ultimately the Congress must resolve any problems that may develop and specify both the degree to which data should be made available from tax authorities, social security, employers, banks and financial institutions and also the procedures and conditions under which such availability takes place. These are not decisions that should be left to program administrators and auditors.

Mr. Chairman, I welcome the attention of the Subcommittee to these complex issues. These hearings are timely. It is urgent that Congress address the need for carefully drawn legislation that will properly balance privacy concerns against the need to obtain the data necessary to ensure program integrity and reduce fraud and waste.

Senator COHEN. Our second panel of witnesses consists of John Shattuck from the American Civil Liberties Union; Robert Ellis Smith, publisher of the Privacy Journal; and Ronald Plesser, who was general counsel to the Privacy Protection Study Commission.

Mr. Shattuck, perhaps we can begin with you.

TESTIMONY OF JOHN H. SHATTUCK, NATIONAL LEGISLATIVE DIRECTOR, AMERICAN CIVIL LIBERTIES UNION, ACCOMPANIED BY NORMA ROLLINS, DIRECTOR, NEW YORK CIVIL LIBERTIES UNION PRIVACY PROJECT; ROBERT ELLIS SMITH, PUBLISHER, PRIVACY JOURNAL; AND RONALD L. PLESSER, FORMER GENERAL COUNSEL TO THE U.S. PRIVACY PROTECTION STUDY COMMISSION

Mr. SHATTUCK. Thank you very much, Mr. Chairman. I'm John Shattuck, national legislative director of the American Civil Liberties Union. I am accompanied today by Norma Rollins, director of the New York Civil Liberties Union privacy project. She will have a couple of comments to make on the New York issue following my statement.

I can't help but observe very briefly at the outset of this, Mr. Chairman, that today is Bill of Rights Day. The Bill of Rights was passed 193 years ago today out of the First Congress. And I think it is a very appropriate day for us to be addressing a very complicated subject that involves major rights issues.

I have a lengthy statement which I will excerpt and summarize. I would welcome questions if you have them during the course of it.

Computer matching provides a revolutionary method of conducting investigations of fraud in Government funds and services because it permits the Government to screen the records of a whole category of people, such as Federal employees, to determine who among them fall into separate, supposedly incompatible, categories, such as welfare recipients. In many respects, this is a commendable goal.

Certainly the goal of eliminating fraud and waste in the Government is very commendable, but, as you've been pointing out repeatedly this morning, Mr. Chairman, the technique of computer matching raises profound issues concerning individual privacy and due process of law, and it also poses serious questions about cost-effectiveness in the internal management of Government programs. Not only that, but I think, as these hearings have demonstrated, the practice of computer matching is growing with very little regulation, and very little information of a systematic nature is available for showing what that practice is all about and how it is working out.

I'd like to back up for a minute though, Mr. Chairman, and look at the effects of computer matching on individual rights in a conceptual way. I think to understand what it is that concerns many of us, it is necessary to grasp the profound difference between a computer and a traditional law enforcement investigation.

A traditional investigation is triggered by some evidence that the target is engaged in wrongdoing. This is equally true for cases of tax evasion, welfare fraud, bank robbery, or traffic speeding, and it is true both because of the limited resources of law enforcement usually make it impractical to conduct dragnet investigations, and more importantly because our whole constitutional system generally bars the Government from investigating persons it does not suspect of some wrongdoing. Of course, audits can always be conducted, but investigations are another matter.

A computer match is not bound by these limitations. It is directed not at an individual, but at an entire category of persons—not because any one of them is suspected of misconduct, but only because the category is of interest to the Government. What makes computer matching so fundamentally different from a conventional investigation is that its very purpose is to generate the evidence of wrongdoing that is necessary before a conventional investigation can be initiated.

With this background, let me turn quickly to four areas of specific individual rights in which I think computer matching is profoundly altering the way in which we look at those rights.

The first involves the fourth amendment. Historically, we all know that the most blatant violations of the fourth amendment have been fishing expeditions directed against large numbers of people on the chance that something will turn up and that they may be guilty of something. In fact, that is what computer matching, on one level, is all about.

The matching of unrelated computer tapes is designed as a general search and is not based on any preexisting evidence to direct suspicion of wrongdoing to any particular person.

Now, it is true, as you've pointed out this morning, Mr. Chairman, that systematic searches of personal records are not as intrusive as door-to-door searches of houses or places of business, but the result is the same—a dragnet into private information about huge numbers of people.

This brings me to the second principle of individual rights that is increasingly at odds with computer matching. That is the presumption of innocence.

Generally speaking, people in our society are not forced to bear a continuous burden of demonstrating to the Government that they are innocent of any wrongdoing. But computer matching tends to turn the presumption of innocence into a presumption of guilt. Let me give a couple of examples.

In Massachusetts, as I will cover a little bit later in my testimony in more detail, welfare recipients have been summarily removed from the State welfare rolls as the result of a computer match. Many are now fighting for reinstatement based on information the State neglected to take into account after their names appeared as hits in the match.

In Florida, the State's attorney for a three-county area around Jacksonville obtained case files for all food stamp recipients in the area, and then launched a fraud investigation against those who received allotments of more than $125 a month, presuming them to be guilty of fraud. The Federal court of appeals 2 years ago invalidated that file search and enjoined the investigation on the grounds that the recipients were put in the improper position by the State of having to prove that the allotment of food stamps they had received was not based on fraud.

The sad fact is, Mr. Chairman, that once a computer match has taken place, any person whose name appears as a raw hit by virtue of turning up on two unrelated computer tapes is often presumed to be guilty of the wrongdoing that is under investigation.

The third, and I think in many ways the most profound, change that computer matching has brought to individual rights involves the Privacy Act. The Privacy Act is intended to establish the principle that individuals have the right to control information about themselves and to prevent its use without their consent for purposes wholly unrelated to that for which it was collected.

The act restricts disclosures by Federal agencies of personally identifiable information such as the kind of information used in computer matches.

There are two major exceptions to this rule. The first involves a "routine use," which is defined as the use of a record for a purpose which is incompatible with the purpose for which it is collected. The second involves a "law enforcement" disclosure which enables an agency to be responsive to a request by another agency for the information relevant to the investigation of a specific violation of law.

Five years ago, Mr. Chairman, when computer matching was in its infancy at the Federal level, the Privacy Act was correctly perceived by several Federal agencies to be a stumbling block. The Civil Service Commission, for example, initially balked at the 1977 plan of HEW Secretary Califano to institute a match of Federal employee records and State welfare rolls on the ground that the use of employee records for such a purpose would violate the Privacy Act.

In a letter which I have appended to my testimony, the Commission's General Counsel stated pointedly that the proposed match could not be considered a routine use of employees' records since the Commission's information on employees was not collected with a view toward detecting welfare abuse.

Similarly, it could not be considered a law enforcement use since—and I quote from the letter—"at the matching stage, there is no indication whatsoever that a violation or potential violation of the law has occurred."

Unfortunately, this candid and honest and, I believe, correct interpretation of the Privacy Act soon gave way to a succession of strained readings by Government lawyers seeking to square computer matching with the act's restrictions on the use of personal records for purposes compatible with those for which they were collected. And since, as my colleague Mr. Plesser will point out, the Privacy Act is left, in terms of its enforcement, almost entirely to the agencies it regulates, it is hardly surprising that the agencies have now miraculously established that computer matching is a routine use of personal records.

In the last 5 years I think the act has been so thoroughly circumvented by the executive branch that, frankly, it can no longer be seen as an effective safeguard against computer matching abuses. But the principle is certainly still there. And that principle underlying the act is that individuals should be able to exercise control over information about themselves. And that principle is wholly incompatible with computer matching.

The fourth and final way in which computer matches change the way in which we look at individual rights involves due process of law. Once a match has taken place, it results in a series of hits, defined in the 1982 guidelines as the identification through a matching program of specific individuals.

At this point, all those identified are in jeopardy of being found to be guilty of wrongdoing. To the extent that they are not given notice of their situation and an adequate opportunity to contest the results of the match, they are denied due process of law. But this is precisely what has happened in several of the best known matching programs conducted to date.

For example, Secretary Califano's operation match results were kept secret from Federal employees whose records were matched with welfare rolls because the Justice Department viewed the investigation—and I quote—"as a law enforcement program designed to detect suspected violations of various criminal statutes."

In Massachusetts, the State welfare authorities have gone one step further in violating due process by terminating benefits to persons showing up as hits without even conducting an internal investigation of the validity and accuracy of the computer match results.

This approach, I think, makes a mockery of both the legal and practical bases for due process of law. Due process is as old as Anglo-American jurisprudence. It is the right to confront one's accuser and to introduce evidence that shows that the accuser is wrong.

When the accuser is a computer tape containing information compiled from government records, the possibility of error is very substantial indeed. I think the kinds of travesties of due process that can result are very poignantly pointed out in the litigation files in the Massachusetts case challenging the welfare bank records match.

I will simply cite one of them which I think is particularly poignant that appears in my testimony. One welfare recipient, a resident of a nursing home, held a certificate of deposit in trust for a local funeral director to be used for her funeral expenses. Her medicaid was ordered terminated when the computer match indicated her bank account was above the medicaid assets limit. This decision is clearly wrong because under Federal regulations a funeral contract account is an exempt resource.

With this kind of background of the profound effect that computer matching is having on individual rights, let me turn next to the question of its regulation or the question of its nonregulation.

At the Federal level, computer matching has been regulated since 1979 by guidelines issued by the Office of Management and Budget. These guidelines, which were revised in 1982, are intended primarily to help agencies—and I quote—"relate procedural requirements of the Privacy Act and the operational requirements of computerized matching." This means that they are intended to paper over the severe and profound incompatibility between computer matching and the Privacy Act insofar as the routine use issue is concerned.

In my view, there is no way to reconcile the Privacy Act with the OMB guidelines. The guidelines represent an effort to work within the procedural framework of the act, while circumventing its substantive requirements.

I think the clearest example of this is the provision in the guidelines setting forth the steps that agencies must follow in planning computer matches. The most important step is to publish a notice in the Federal Register defining the proposed match as a routine use of the records to be compared.

The guidelines state that the notice should explain the justification of the routine use, including how the disclosure is compatible with the purpose for which the information to be matched was collected. There is no way this requirement can be satisfied since the matching of unrelated records will necessarily be unrelated to the purposes for which they were originally collected.

Apart from this tortured effort to rationalize computer matching with the Privacy Act, I think the OMB guidelines provide a few restrictions on matching programs. But the minimal list of protections is greatly overshadowed by the fact that the guidelines contain no requirements or limitations on the conduct of matching critical areas.

The first area on which the guidelines are silent is the nature of the record system to be matched. So far as I can tell, no personal records, no matter how sensitive—medical files, security clearance records, et cetera—are beyond the reach of computer matching for any investigative purpose whatsoever under these guidelines.

The second totally unregulated area involves the procedures to be followed in determining the validity of hits. There are no prescriptions in the guidelines for what is to happen after a hit has been reached. And presumably the same kind of tragedies that are now occurring in Massachusetts could well occur at the Federal level, and may well have occurred in areas that I'm not aware of, because there are no procedural due process requirements that are spelled out.

The third major area missing from the guidelines involves the standards and procedures to be followed for securing OMB approval for a proposed match. Here again, I am not aware of a single instance in which OMB has declined to approve a match. In fact, as far as we can tell, OMB would just as soon, as you say, get out of the picture entirely. So there are no standards or procedures.

Senator COHEN. The committee has no record of OMB ever rejecting any proposal to match.

Mr. SHATTUCK. The final thing, Mr. Chairman, is that the guidelines made no mention of the projected costs and benefits of the proposed match, as well as the actual costs and benefits of those matches it conducted.

As Senator Levin pointed out, that is a major engine rule of possible regulation, were it to be incorporated into the guidelines. It was in 1979, taken out in 1982.

So, I think, for all these reasons, it is difficult not to conclude that computer matching is a totally unregulated business at the Federal level and presumably, similarly, at the State level.

Now, I would like to just briefly summarize two specific matches that have taken place, which I think illustrate all of the problems that I am talking about here this morning.

I will skip over Project Match, because I think a good deal of ink has been spilled on that subject, and it's not necessary to cover it.

But I'd like to talk briefly about the Selective Service and IRS match which is underway right now, because I think it shows the great danger here.

Under this program, IRS is using its computers to match addresses in its files with the names of 250,000 individuals supplied by the Selective Service System, all of whom will eventually receive notices that they face possible prosecution if they fail to register and that their addresses may soon be provided by IRS to Selective Service.

The issues raised by this match I think illustrate the danger, the great danger of using the records of a particularly sensitive and unique agency such as IRS in any matching program, especially one with such a clear prosecutive purpose.

First, the match involves IRS in a matter wholly unrelated to the enforcement of the tax laws, which depend, in large measure, on the willingness of taxpayers to provide large amounts of sensitive information about themselves.

Second, the match raises the specter that the tax records of those receiving the IRS letter will receive special attention because of their suspected status as nonregistrants.

Third, the match seriously erodes taxpayers' confidence in the privacy of their tax records and the independence of IRS.

All of these related dangers I think could have a devastating impact not only on the rights of taxpayers but on the function of the Internal Revenue Service and the operation of the Federal Government in that area.

Senator COHEN. Mr. Shattuck, could I interrupt you here, because we're getting into an area which requires some need to distinguish all the lines.

What about the IRS supplying information to drug enforcement agencies?

Mr. SHATTUCK. Mr. Chairman, I'm what I guess Mr. McBride would call a purist in this area. When it comes to the records of the Internal Revenue Service, I do not believe any such records should be provided to other agencies outside of the framework that is set up by the Tax Reform Act of 1976.

Senator COHEN. What if you can demonstrate that there are large amounts of drugs coming into this country from drug dealers who are not paying taxes?

Mr. SHATTUCK. I think the court-ordered procedures of the 1976 act are available for the Justice Department to obtain records of persons who might be suspected in this area.

But as far as the generalized matching of IRS records and drug enforcement records, I would oppose that, because I think if you open the door of the IRS to one agency, you're going to have a lot of others lining up for equally compelling purposes.

And I think not only the taxpayers' privacy will suffer, but the IRS will as well.

Let me move to the second major area of specific examples though before I conclude my testimony. And that is at the State level.

I mentioned Massachusetts several times here this morning, and I will go into that for a couple of minutes.

And my colleague, Norma Rollins, who has presented a report to the committee concerning the New York situation, will have a couple of comments to make about that.

Massachusetts' welfare-bank records match began in August 1982. The State department of public welfare submitted computer tapes bearing the social security numbers of all welfare recipients in the State to 117 Massachusetts banks, having a total of 7 million deposit accounts.

By comparing the social security numbers with bank account records, the banks were able to identify for the State all the welfare recipients who had cash assets beyond the allowable limit for persons on welfare.

Upon receiving these lists of hits from the banks, the department of public welfare did nothing further to check the accuracy of the assets' information or determine its relevance to the eligibility of particular recipients. Instead, it immediately sent out benefit termination notices to all those whose names appeared as hits.

The problems associated with this rather typical kind of match are many.

First, the use of bank account information raises many of the same far-reaching questions of confidentiality that I believe are raised by tax records matches. Information from bank accounts is never intended to be generally available to Government investigators for the asking, as I think is emphasized by the Federal Right to Financial Privacy Act which passed in 1978, which generally requires court procedures or subpenas or administrative summonses for access to bank records.

Second, the sending of termination notices to all welfare recipients showing up as hits on the match constitutes a denial of due process of law and a costly and inefficient method of managing the welfare system.

There are many ways in which the presumption of guilt created by a hit on the match could be erroneous. As we saw in the litigation challenging that Massachusetts match, the assets in the account may not be the property of the welfare recipient. The assets may be legally justifiable, for example to pay funeral expenses, the account may be held jointly by several people, et cetera.

In any event, the error rate for welfare terminations based solely on these computer matches appears to be exceptionally high, as shown by the fact that appeals are now being filed at six times the ordinary appeal rate of people whose benefits have been ordered to be terminated.

And I think that simply constitutes not only an improper match, but a rather mismanaged welfare system, which then has to deal with six times the number of appeals and terminations which otherwise would have never occurred.

Third, and perhaps most important, I think, the Massachusetts program demonstrates how utterly ineffective the computer match is in providing the kind of detailed, credible and verified information that is needed to reach a conclusive judgment as to whether a person is eligible for welfare or has committed welfare fraud.

As you pointed out earlier, Mr. Chairman, no human element is involved in this match of complicated sets of records to make the kind of complex judgments that are needed.

For example, judgments are complex because each welfare program exempts certain types of assets in determining eligibility. It's not possible to simply state that because someone has gone above a certain level in the bank records that they're going to be guilty of welfare fraud.

I am all in favor of the streamlining of eligibility requirements in the welfare system. I think that would certainly serve to improve the management of most welfare programs. But that hasn't happened in many areas. And the complexity of these requirements I think renders both inadequate and dangerous the kind of simplistic hit information provided by the Massachusetts welfare-bank record match.

Let me just conclude, Mr. Chairman, by making a couple of specific recommendations and observations, following your suggestion that this subject may be ripe for legislative action.

I think computer matching is a very attractive investigative technique. It's particularly attractive because it appears, for the first time, to permit law enforcement officials to instantaneously root out all instances of a particular kind of wrongdoing in a particular segment of the population.

It provides for, as Mr. McBride was saying, a very nonintrusive general surveillance system, which supposedly can detect and observe misconduct wherever it is used. And it appeals, I think, to the perfectly reasonable adage that if you haven't done anything wrong, you don't have anything to worry about. But I think the costs are very high. The costs for individual rights are particularly high, and the other kinds of costs we're not yet that clear about.

But the main thing is that the data can often be inadequate or inaccurately reported. It can present a very incomplete picture of the persons to whom it pertains. It is very unlikely to be sufficient to answer difficult questions of whether a person is entitled to receive welfare or is engaged in a conflict of interest, or what have you. On the other hand, I think it almost certainly erodes all of the various rights.

So, I would make as a general framework of recommendations, Mr. Chairman:

First, the Privacy Act should be amended to clarify that computer matches are not routine uses of personal records.

Second, no further Federal computer matches should be permitted without express congressional authorization.

Third, the Congress should not authorize computer matches of sensitive personal records, the confidentiality of which is otherwise protected by statute, such as taxpayer records, census records, bank records, or similar records.

I think no computer match should be authorized until an analysis has been made of its projected costs and projected savings and the recoupment of funds owed to the Government and a determination has been made that the public benefit will far outweigh the cost, and that individual rights will be protected.

Finally, Mr. Chairman, I think procedural due process protections for the persons whose records are being matched should be specified by statute, including the right to counsel, the right to a full hearing, and a right to the confidentiality of results.

These are only tentative and preliminary recommendations. But I think the thrust of them, frankly, is to say let's have a moratorium for some time, study this very complicated and far-reaching issue, which no doubt, in terms of the value of computer matching in some areas, Congress may determine, based on a great deal of information, that it is valuable. In many other areas, I think it's going to find that the abuses are so significant as to bar the technique from being used.

But in any event, the time is certainly ripe for studying and very soon, hopefully, for legislating.

Thank you very much, Mr. Chairman.

If I may, perhaps I could permit my colleague, Ms. Rollins, to briefly summarize the results of the New York procedure.

Senator **Cohen**. Ms. Rollins.

Ms. **Rollins**. My report has already been appended to Mr. Shattuck's testimony.[1]

The report is a result of the New York Civil Liberties Union review of the figures published by the New York Department of Taxation, Labor and Special Services in their joint annual wage reporting systems report.

We have also reviewed the 1982 New York State budget allocations for these agencies. Our examination leads us to believe that, in spite of the claims of millions of dollars saved by these agencies, that WRS is not cost effective and that the privacy of millions of New Yorkers has been endangered, to very little purpose.

Specifically, our analysis of the claims made for the wage report systems suggests the following:

That the actual cost of operating the system is far greater than New York State admits; that there are many hidden costs to employers which have not been computed; that estimates of savings include millions of dollars that, in fact, cannot or will not be saved; and that losses to public assistance and unemployment programs attributable to deliberate fraud and abuse could be detected by less cumbersome and wasteful means.

The reported annual costs of WRS are approximately $6 million. However, we believe this represents only a very small portion of the cost of operating the system, because only a portion of the actual costs attributable to WRS are identified as such.

For example, neither in the WRS report nor in the New York State budget is there a special WRS appropriation for the Department of Labor. How can it be possible for the Department to participate in the cross-matching of over 1.2 million records and audit nearly 67,000 cases without spending one penny?

We further believe that the largest unaccounted cost is represented by the many thousands of hours required for administrative case work in the local department of social services district offices to review, verify, and investigate approximately 90,000 "hits" cases every quarter. No budget allocation was made for this, nor was its cost included in the annual report.

---

[1] See p. 436.

In addition to hidden costs directly undertaken by State agencies, there are the costs of the system by the more than 325,000 employers filing wage reports on 8 million employees each quarter. Submission of wage data is not the only responsibility that WRS imposes on employers.

Followup investigations on hits require employers to respond to numerous requests for detailed employment histories. For example, the New York City Human Resources Administration asks the employers to provide 2 years of employment history for every recipient reviewed.

Even if the burden on the individual employer is modest, the combined annual contribution to the operation of WRS for New York's 325,000-plus employers and unaccounted costs can easily come to $30 million.

The department of social services claims WRS is responsible for saving $23.7 million in 1981. However, how much is actually saved depends on how long payments would have continued at their earlier levels.

The department routinely projects savings on each case closed or rebudgeted for 18 months into the future. In fact, however, there has always been a high turnover in public assistance recipients. It's seriously misleading to absorb cases closed in one fiscal year into a gross savings in the next. Just as it is a mistake to assume that closed cases would have remained open, so is it a mistake to assume that a case once closed will remain so. The department has not disclosed how many cases are reopened or how many decisions to close had to be reversed.

With regard to the Department of Labor, more than two-thirds of the reported savings consist of future benefits forfeited. But these savings would only be realized if all the affected individuals were to come forward to claim further benefits.

We do not dispute that the system has produced savings in the public assistance and unemployment programs. We question, however, whether some of the millions of dollars claimed as savings represents money truly saved and note that the published data is not sufficient to permit an accurate judgment.

Computer matching is not a simple or efficient operation. In the department of social services, between 1.2 and 1.8 million records are matched each quarter, producing hits in about 10 percent of the cases. About one-half of these hits, or about 100,000, are sent back to the local districts for a painstaking investigation, often requiring multiple contact with the clients and employers. The paperwork is formidable, yet the number of cases finally affected is minute.

Of the 1.5 million cases examined in the last quarter reported, 2,675 were rebudgeted or closed, but only 86 of those, because they were found to be ineligible for benefits. And even in those cases, we don't know how many involved fraudulent claims.

Perhaps this system may be better than nothing, but how does cost control by computer matching compare to other methods? Do random audits produce equivalent results? Could DSS devise internal adminstrative accounting measures that would provide more reliable indicators of possible fraud? Might not fraud and waste be reduced even more by simplifying the rules for examining eligibility?

The mystique of computer matching has achieved widespread appeal. The apparently simple procedure of matching two data bases and spitting out hits seems like a logical and scientific answer to a complex management problem. We submit, however, the wage reporting system in New York is an extraordinarily clumsy and wasteful operation, and it costs far more and saves far less than its proponents claim, and its impact on privacy cannot be justified as a cost-effective means of controlling fraud and abuse.

Senator **Cohen**. Thank you very much.

Perhaps I could just clarify something before going to Mr. Smith and to Mr. Plesser. I think perhaps my remarks may have been misconstrued, Mr. Shattuck, about the nonobtrusiveness of computers. I see that as a siren song. The very appealing notion that the computer is less intrusive, to me, makes it that much more insidious. I don't see that as a benefit, although it may have the appeal of saying this is not really searching your person or rummaging around through your records by some character in a raincoat in a dark cap who is following you around. It has a very insidious character to it, and I don't feel, for example, any more secure that my conversations might be picked up by satellite instead of a spike mike or an old obsolete telephone tap.

The fact is that, with technology, we are able to achieve those remarkable kinds of performances through scientific discovery. I prefer some sort of intrusiveness. I would prefer to have a man checking the records or going to my bank and making requests, because at least I have a notice that someone is interested in my affairs, at least I have an opportunity to complain to somebody, at least I have an opportunity to file a lawsuit or, God forbid, call my Congressman; right? Or write my Congressman or Senator. At least when you are aware that things are being done, you have some recourse.

What is particularly dangerous, I think, under the appealing character of it being less intrusive, is the fact that all of your documents, all of your most confidential private information is being scanned through this massive computer. That, to me, is one of the real dangers that we need to focus upon, to somehow make sure that we continue to bring human beings into the process.

That is the reason I mentioned the social security disability cases that Senator Levin and I have been so involved within the past 6 or 8 months. You have a situation where cases are being selected for review by the computer, and we have people who are in iron lungs, or body casts, being terminated from disability, or somebody who is blind in one eye and has tunnel vision in the other and can't walk without assistance, being terminated.

This goes on because there has been no person involved in face-to-face contact, and I think that's something we've got to be very, very concerned about with these computer matches, authorizing their use, and setting standards to make sure that somebody is watching, other than just simply feeding information in and taking information out and cross-matching it. Because I think that old expression, "If you sacrifice your liberty for your life, you're liable to end up with neither," may be true here. If you sacrifice your privacy for efficiency, you're quite likely to have neither. What we have to have is that balance.

I very much welcome your remarks, Mr. Shattuck, and they will also be matched with those who have gone, to see if we can't come up with some sort of legislative solution.

Mr. Smith?

Mr. SMITH. Thank you, Mr. Chairman.

I think the oversight function is very important. Congress anticipated that in passing the Privacy Act of 1974, first thinking that some sort of Federal commission could do that, realizing that privacy questions are a matter of balance. They aren't absolute.

When it was decided that we ought not add to the Federal bureaucracy, that function of oversight was delegated to the Office of Management and Budget, so that these questions could be resolved. I think you are very right to identify as one of these problems, that inspectors general themselves are making the decisions without any impartial tribunal to decide some of the countervailing cost effectiveness and privacy arguments.

In the Privacy Act, Congress declared, as a matter of national policy, that exchanges of personal data among Federal agencies ought to be discouraged, and they permitted them only with certain specific exceptions. It seems like an illogical conclusion that information held by one agency ought not to be used by another for purposes of this sort, but it was thought then that the Nation was better off by recognizing that an individual makes a compact with the Government when he deals with one Federal agency, supplying information on the understanding that it will not be used for some other purpose.

Among other things, this increases the candor and honesty with which people submit information to their Government.

Three years after the act was passed, the Department of HEW, in a highly publicized move, originated a match program. Two years after that, the Office of Management and Budget came up with guidelines and for the first time required Federal agencies to at least think twice before conducting these matches and, among other things, decide whether the costs are outweighed by the possible benefits.

In May 1982, even those rather lenient safeguards were repealed. Now for the first time, the Congress is actually taking a look at whether these matches are in the best public interest. I am pleased—even though it probably should have been done before the matches were conducted—I am pleased, at any rate, that oversight is occurring at this time.

Mr. Kusserow, in meetings with his colleagues in the Federal Government, said, in fact, "matches" are misnomers. They ought to be called "editing functions." These matches do no more than "cleanse the data base." But, in fact, some real human agonies are involved. If this were no more than an editing function, I think no due process, no privacy rights would arise. But, in fact, the editing function is knocking people off entitlements that they otherwise would have.

There were some examples of this in the original Project Match done in the 1970's at HEW. When all the dust had cleared, only 15 cases were referred for indictment, involving HEW employees who were also on the computer list of the welfare department. Of the 15 mothers involved, 1 woman's case is particularly instructive. She had quit nursing school when told by her doctor that she had cancer. After months of treatment, she convinced the doctor to let her go back to work. She found a job with an HEW agency, St. Elizabeth's Hospital, and twice, not once but twice, she notified the welfare agency that she had found work. As so often happens in these cases, some well-meaning social worker told her, "Probably a computer will continue to send you checks for a while. Don't worry about it." So she didn't, but after the checks kept coming, she found it irresistible not to cash those checks and use them for medical expenses.

I am not justifying that, but I am trying to show that typically in these cases, it is the Government that continues to tempt welfare recipients by sending the benefits even after notified that the person is no longer eligible.

She was called out of her job and confronted by three investigators from HEW, and when she tried to explain the situation, she was constantly told, "This is a big priority with the Secretary, and you are in deep trouble because of Project Match."

So she quit her job. I'm not sure that is in the interests of the Government, but she quit her job. Three months later, friends called to tell her that her name was in the paper, because the Secretary of HEW had proudly displayed the names of 15 welfare mothers whom his Project Match had turned up as also holding jobs.

I think, incidentally, it is curious that most of these matches to date seem to be going after the working poor. I would think that a much larger priority ought to be people who are getting duplicate welfare checks and qualify for only one.

The match in New York and New Jersey, in which the welfare rolls of one State are compared to another, in my mind, raises no privacy issues, because the information in both cases is provided for a compatible purpose.

Those are the matches that would seem to me to turn up the real bad actors, not matches that are turning up people whose bank accounts are slightly over a certain amount, or those ironically who are fortunate enough to find employment.

This woman was about to plead guilty on the advice of her court-appointed attorney, and the Judge, Judge Gesell, spoke up and asked her whether she notified the welfare officials about finding employment. She said that she had, so he threw the case out of court.

This case illustrates——

Senator COHEN. Did he throw her court-appointed lawyer out of court too?

Mr. SMITH. I didn't hear that, sir.

Senator COHEN. Sorry. Go ahead.

Mr. SMITH. This is an accurate match, but there are thousands of inaccurate matches, because those who have been in the computer business know that the best laid data processing plans always go astray.

I was interested to sit in on some meetings of those who are conducting the match programs, who pointed out pitfalls. These programs invariably use great reliance on the social security number, which we know is not a reliable identifier. There are lots of duplicates around the country. There are lots of people with more than one number. There are lots of numbers that are inaccurate because of mistakes or because of fraud. In study upon study in the legislative history of the Privacy Act, we have had indications that this drift toward a national identifier ought to be discouraged. Match programs, by definition, continue to accelerate this trend. The representative of the Veterans' Administration pointed out to his colleagues that information gathered by one agency may not be verified at all, because it means nothing to that agency. Date of birth on an application for a farm loan, for instance, means very little to the farm agency; so they don't verify the information. When that information is used as the basis of a match, it takes on added importance.

The same is true of social security numbers gathered by banks. The banks really don't care about the accuracy of those numbers. It is the Internal Revenue Service that cares. So that information is simply passed on to the Government without any verification.

Now in Massachusetts, that information takes on crucial importance, because the welfare department is using it as the basis for a match, and this is exactly what Senator Ervin pointed out in the deliberations on the Privacy Act. The reason why exchanges among Federal agencies ought to be discouraged is precisely because one agency gathers information that it may need at some later time and is not particularly excited as to whether the information is accurate. It simply leaves it in the file. And there ought to be some means to verify that information to make sure it is accurate, before it is used in any exchange with some other Federal agency.

Senator Ervin pointed out that the routine use part of the act was intended to accelerate certain housekeeping functions, but he made clear, however, that it was "intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material."

In Massachusetts, we have, as has been pointed out, a match involving the banks. One thing that can be said about this match is that it is pursuant to law. I really think most matches being conducted across agency lines are clear violations of the Privacy Act.

Senator COHEN. The Privacy Act, as I understand it, doesn't apply to the States.

Mr. SMITH. That is correct. This match is being conducted in compliance with the law. As much as I may dislike it, there is a law on the books in Massachusetts which authorizes this match with the banks. And what they are doing is matching to see which welfare recipients might be above an arbitrary ceiling in their liquid assets in a bank. Termination notices are going out on the basis of machine matches without any followup questions.

I remember a Supreme Court case about 5 years ago, *Memphis Light, Gas & Water Division* v. *Croft*, that might be relevant here. It indicated that machine matches are not adequate for terminating benefits or service. There has to be some human intervention. But in Massachusetts, notices are going out based on the computer match. Here are the results so far of those who have been called in for hearings. Out of 251 persons called in for hearings on the basis of simply a match that showed that their social security number matched the social security number of a depositor who had an account over a certain amount, usually $1,000 or $2,000, 110 of those 251 hearings were found in favor of the recipient. So the batting average on this match is not very high.

Of those hearings in which the recipient prevailed, 46 prevailed because there were errors in social security numbers or names that could have been verified by simply looking at the manual file that the welfare department has in its control. Fourteen of those persons spent the money or closed down the account between the time the match showed them in violation and the time a termination letter was sent out.

I am not sure that that's in the interests of the Government either, encouraging people to spend money to stay on public assistance if it's needed.

Senator COHEN. We do it all the time at the Federal level. We have what we call "hurry-up spending." All the agencies spend their money as quickly as they can at the end of the year, to make sure Congress doesn't reduce the level of appropriations the following year.

Mr. SMITH. The end result of this match, I think, is that it is not in the public interest. People are encouraged to be duplicitious and put their money elsewhere or spend it. In fact, there were 41 individuals who lost the hearings, because they didn't spend the money quick enough. They did spend down their accounts, but after the termination notice went out. So just because of a number of days, some 41 were losers and some 14 were winners.

Of those 41, most are simply going to reapply for benefits, go through the procedure once again, and have bank accounts under the ceiling; I'm not sure that that's in the public interest either.

There were a couple of cases in which the bank accounts were over the limit by $7. So against this human agony we must weigh the Government's claims to vast savings with this computer match.

I feel I am not in a position to evaluate the cost effectiveness, but I think the data is available, it ought to be scrutinized. In each case the savings assume that the money that would naturally flow to the recipients for the rest of his or her lifetime will be recouped by the Government; it assumes of course that the hit will be confirmed and the violator located, and that the violator has no defense, and that the Government in fact can prove its case.

I say there are too many "ifs" involved and the subcommittee can use the data which is available to see whether these matches are cost effective.

I want to emphasize that even if matching is cost effective, I think that it raises very real problems with regard to violations of the Privacy Act—and as John Shattuck has pointed out, certainly the philosophy of the fourth amendment, if not the actual words of it. However, there are certain computer matches, I think, that we can all agree on as being legitimate. Those would include matches of lists of known dead persons. Case law shows that the right to privacy dies when the individual dies.

Also matches involving data within one particular agency; also matches that are prompted by a suspicion of wrongdoing, as is in the case of suspected fraud. I think the Privacy Act law enforcement exemption certainly does cover that eventuality.

Does all this mean that the Government is defenseless to fight fraud? I think not. I was interested in my research to discover two reports from the Government itself, which said, in the first instance, the match program seemed to be looking in the wrong places; and second, that these matches are not the best technique for getting the fraud that exists.

The Attorney General's Federal Advisory Committee on False Identification in 1976, in which I participated, found that one of the greatest problems in welfare waste and fraud was at the identification stage when the individual applies for benefits. It said that Federal and State agencies don't have a good idea of who is receiving welfare money in the United States.

Senator **Cohen**. Mr. Smith, I encourage you to try and summarize as quickly as you can, because we've got to get to Mr. Plesser, and we're rapidly running out of time.

Mr. **Smith**. Fine. A second study which was ordered by the Department of Justice showed all sorts of other techniques that the Government could use to get at the problem of fraud and waste, and it didn't mention throughout anything about computerized matches.

The subcommittee can encourage the Government to look at some of these other techniques that do exist and that do not raise any questions about the Privacy Act. I'm not sure that the act needs amending—I may disagree with my colleagues on that. I'm reluctant to open it up to amendment.

I think the routine use and its legislative history couldn't be clearer. If there is a means for the subcommittee to emphasize that routine use is not intended to cover all matching situations, I think that would be very much in the public interest.

I would like to respond to two aspects of Mr. McBride's testimony; first, that the Congress somehow accelerate the use of the social security number. There's adequate information on the record from Senators Percy and Goldwater as to why this would not be in the public interest.

Second, he would suggest legislation to increase the reporting of wage data to the States—the eight States that don't report quarterly. We have a big push toward savings on paperwork. Just 3 or 4 years ago, one of the prime accomplishments at that point, they told us, was reducing the amount of reporting to the States. So are we going to reverse ourselves and tell the States to start reporting quarterly instead of annually?

Senator **Cohen**. I don't think Mr. McBride suggested we ought to accelerate the use of social security numbers. I think what he said was that he was uncertain to what use social security numbers may be put, and he thought a thoughtful examination of where we're going with social security numbers in being identifies number would be good for everybody.

Mr. Plesser?

Mr. **Plesser**. Thank you very much, Senator Cohen. I will try to summarize my comments because I think my colleagues this morning have done a very good job in pointing out the problems with matching.

I have two points that I would like to make in the context of the Privacy Commission. I was general counsel of the Privacy Commission, and we saw some of these problems coming. We had a very difficult time conceptualizing whether an individual has a right in our society to control how information is used about that person.

Our deliberations were made a lot easier, unfortunately, at the expense of the public interest, by the Supreme Court in 1976. The superior court came out with a case called *Miller* v. *the United States,* and *Miller* while not directly involved in matching, I think, still has validity in that it said, one, that the fourth amendment has no relevancy in the information privacy arena; that is, where a third party is maintaining information about you, the fourth amendment provides you almost no protection.

Mr. Miller's bank accounts were readily available to agents of the Treasury Department. He attempted to raise some very straightforward procedural problems when these agents had failed to issue proper subpenas. In response, the Supreme Court said Mr. Miller had no interest in his bank records and that those bank records were the property of the bank. The court reasoned that as soon as Mr. Miller entered into commerce, he lost whatever interest he had, and the fourth amendment doesn't apply to protect those records against unreasonable searches and seizures.

Congress since that time, as John Shattuck earlier this morning has mentioned, has enacted something called the Right to Financial Privacy Act, which to a limited extent tried to solve Mr. Miller's problem. But that legislation does not alter the basic holding of Miller that the Constitution doesn't assist in the protection against Government access to computer records.

So what does that all give us? That gives us—the Constitution really, unfortunately, isn't very helpful. The idea of the fourth amendment—you said it almost better than I could say it, Senator, when you said that a search by match is almost as bad as a man-in-the-house search. It is really no different in historical perspective, in having an agent come in and rifle your papers. Somehow the computer has sanitized that search. The computer—the technology—has made it OK.

I don't think there's much difference and I think that the framers of the Constitution when faced with this question would have found that the fourth amendment should be applied to information privacy where a third party is in possession of information.

That leads us to what are the legislative kind of protections that we have. If the Constitution isn't very helpful, what are the legislative protections?

If I can look at the Privacy Act for a second, I don't disagree with my colleagues that the routine use provision is probably being violated, I would want to emphasize that I think the routine use provision as written allows for broad interpretation, and agencies have gone all the way to try to create the broadest interpretations that they can.

We say, OK, if those interpretations are overbroad, where are the mechanisms to control them? Like every agency under most statutes, they try to read legislation favorable to them. But generally there are mechanisms in which other forces or other interests in time control that.

Well, let's look at the Privacy Act. The Privacy Act, to my experience is essentially unenforceable in this kind of area.

The reason for that is very simple. The Privacy Act has been interpreted by several courts to exclude injunctions under the Privacy Act. Well, if you can't stop the Government from doing something that's wrong. What can you do?

You can get damages after the fact. In order to be able to obtain those damages, a plaintiff must show that the agency acted willfully or intentionally to violate the act, which is a fairly strong standard; and that you have to demonstrate that the individual or you have been adversely affected. I've just been through a court process, not in the matching program but in a similar program, and I've attached to my testimony an opinion in that case which I think demonstrates these problems.

Just that the agency did a wrong is not enough. Just the case that they violated the law is not enough: there has to be a demonstration of adverse effect. And then if you can get through those hurdles, the only thing you can recover is actual damages.

That has been interpreted as out-of-pocket loss. So that emotional harm, loss to reputation—any of the traditional kinds of damages associated with, say, libel cases or first amendment invasions, have been thrown out the window.

I had a U.S. district court judge three blocks from here tell me 3 weeks ago that my clients could only recover in a Privacy Act case if I showed a substantial physical injury. Now I ask you. What is a substantial physical injury in a Privacy Act violation? Does a computer reel have to throw off and hit somebody in the face?

To bring it back to match, I think much has been made in the guidelines and the OMB about the Privacy Act is going to hold the tide on this. I don't think that's right.

I agree with Bob Smith that the routine-use provision meant something when it was written, and that it should mean something. But there's no way to enforce it, and laws that aren't enforced—and are not enforceable—are really of very little use.

I think that's really my major message, and I want to tie that with what I think the overall tragedy of match is, which is that there's no countervailing constituency for privacy in the Federal establishment.

Mr. Kusserow does a fine job; he has 1,000 employees working in his office. There is probably one person in HHS whose job it is to look at privacy. There's only one agency that I know of that really institutionalizes privacy and that's the Department of Defense. They've had a Defense Privacy Board—it's absolutely true, they have a Defense Privacy Board—with high-level civilians and officers. I don't always agree with what they do, but they're there and they're watchdogs.

There is no equivalent watchdog in any other agency. The Privacy Commission recommended a cap watchdog Federal agency of a small but permanent nature to look at these issues. The Carter and Reagan administrations did not follow those recommendations; as a result of their interests in decreasing the bureaucracy, which is also a counterbalancing interest, but unfortunately, there's no one in the Federal Government, and the role falls to Senate and House committees to do the oversight. And while I applaud the oversight, I think there should be some administration oversight before it gets thrown into the laps of Congress.

Thank you.

Senator COHEN. Thank you very much, Mr. Plesser. I happen to agree with your last point in particular. In Congress, as much as we try to exercise oversight, it's very sporadic and is subject to the call of the bells. It's subject to four other committees and nine subcommittees and we simply don't have the ability to monitor or to oversee these kinds of activities and violations of our rights.

Frankly, I think we're rapidly approaching a society in which the human voice is not going to be able to be heard above the whir of that computer, and that is very troubling. And it ought to be troubling to everybody. But technology is something we're fascinated with, and we all see the danger down the road.

I think back to my days of practicing law; the case I recall was *Mapp* v. *Ohio,* the classic unreasonable search and seizure; and those stomach-pumping cases where they would go after evidence that you had swallowed and get it out of you. While this is a much more sophisticated problem, we have a much more sophisticated society in which we get almost as much information gathered very discreetly and surrepticiously than we'll ever know about.

And I think that we've got to devise some sort of check against that. But more importantly, the purpose of the hearings hopefully, as well as providing for legislative solutions, is to sensitize people to what is going on, so that at least we have the opportunity to voice our concerns and to discuss it freely before we seem to become sort of immune to it all.

What difference does it make as long as the information is being collected? You have nothing to hide, if you're honest, don't worry about it. Because I don't think we could have projected 10 years ago the uses to which the computer is going to be put, and if we had to project 10 years into the future depending on what government happens to be in place, the kind of information that will be cataloged and carried, not destroyed—and the profile being disregarded but kept, maintained, and constantly being put into different matches or cross matches to determine all kinds of things that we presently don't even consider to be conceivable in a free and open society.

So I think the hearing, if nothing else, will at least serve to put the public on notice that there's a serious issue here: there are serious problems associated with it and that individual liberties are in danger of being eroded unless we have standards in oversight and checks, and most important, disclosure.

I even find the OMB guideline about publishing a matching notice as reasonably close to the match being made not being followed. The match was made back in August on student loans, and you didn't read about it in the Federal Register until December, and only because we were looking for it at that particular time. That's not even applying the relaxed standards we have today.

So I thank all of you for coming. We have 1 more day of hearings tomorrow to deal with these issues, but hopefully it won't be the end of it because we just had 2 days of hearings.

Hopefully it will serve as at least a first step for the next Congress coming in, but if we simply hold hearings and take no action, it'll disappear into just another series of hearings by another committee. Life will go on, and these problems will continue to be ignored. So I thank you all for coming.

[The prepared statements of Mr. Shattuck, with attachments; Mr. Smith; and Mr. Plesser, with attachments; follow:]

PREPARED STATEMENT OF JOHN SHATTUCK

Introduction

I am pleased to appear before the Subcommittee on behalf of the American Civil Liberties Union to discuss the use by government agencies of a rapidly growing new investigative technique: the matching of unrelated computerized files of individuals in order to identify suspected law violators. This technique--"computer-matching"--provides a revoluntionary method of conducting investigations of fraud, abuse and waste of government funds because it permits the government to screen the records of whole categories of people, such as federal employees, to determine who among them also falls into separate, supposedly incompatible categories, such as welfare recipients.

Computer-matching raises profound issues concerning individual privacy, due process of law and the presumption of innocence. It also poses serious questions about cost-effectiveness and the internal management and audit of government programs.

The ACLU is a nationwide, non-partisan organization of more than 250,000 members dedicated to preserving and enhancing rights guaranteed by the Constitution. We bring substantial experience and commitment to issues of individual privacy, having been at the forefront of efforts in the Congress over the last decade to enact privacy legislation, notably the Privacy Act of 1974, the Tax Reform Act of 1976, the Right to Financial Privacy Act of 1978, and the Privacy Protection Act of 1980. My own experience in this area is based on five years of service as counsel to the ACLU's Privacy Project and five years as national legislative director of the organization, as well as the authorship of a college textbook, Rights of Privacy (National Textbook Company, 1978) and a variety of studies and articles on information privacy issues.

In my testimony I will review the major constitutional and legal principles which I believe are being undermined by the increasing and largely unregulated conduct of computer-matching investigations. I will then comment on the two sets of federal guidelines promulgated in 1979 and 1982 by the Office of Management and Budget concerning computerized matching programs, neither of which in my view reflects any serious consideration of privacy principles nor contains adequate protections and safeguards against abuse. I will review several specific examples of recently conducted computer matches that pose threats to individual rights, and I will summarize information on the public record about the cost-effectiveness of some of these programs. Finally, I will set forth several alternatives to computer-matching for curtailing fraud and waste in the administration of government programs, and I will recommend several legislative and regulatory measures to control and limit the use of computer-matching in the interests of safeguarding individual rights.

Effects of Computer-Matching on Individual Rights

To understand the impact of computer-matching on individual rights, it is first necessary to grasp the profound difference between a computer-match investigation and a traditional law enforcement investigation.

A traditional investigation is triggered by some evidence that the target has engaged in wrongdoing. This is equally true for cases of tax evasion, welfare fraud, bank robbery or traffic speeding, and it is true both because the limited resources of law enforcement usually make it impracticable to conduct dragnet investigations and, more importantly, because our constitutional system generally bars the government from investigating persons it does not suspect of wrongdoing.

A computer-match is not bound by these limitations. It is directed not at an individual, but at an entire category of persons, not because any one of them is suspected of misconduct, but because the category is of interest to the government. What makes computer-matching so fundamentally different from a traditional investigation is that its very purpose is to generate the evidence of wrongdoing that is required before an investigation can be initiated. That evidence is produced by "matching" two sets of personal records compiled by the government for wholly unrelated purposes.

There are at least four ways in which a computer-match differs from a conventional law enforcement investigation in terms of its impact on individual rights:

1. Fourth Amendment

The Fourth Amendment to the Constitution protects against unreasonable searches and seizures, the most blatant of which historically have been "fishing expeditions" directed against large numbers of people on the chance that "something will turn up." From the "writs of assistance" that were used in the 18th century by royal revenue agents to search door-to-door for violations of the British tariff laws in the American Colonies[1] to the municipal code inspections used in the 20th century to enforce health and safety standards,[2] the principle that generalized fishing expeditions violate the right to be free from unreasonable searches and seizures has held firm in American law.

That principle is violated by computer-matching. The technique of matching unrelated computer tapes is intentionally designed as a general search and is not based on any pre-existing evidence to direct suspicion of wrongdoing to any particular member of the category of people whose records are to be matched. While it is true that systematic searches of personal records are not as intrusive as door-to-door searches of houses or places of business, the result is the same: a massive dragnet into the private affairs of huge numbers of people.

---

[1] Lasson, *The History and Development of the Fourth Amendment* (Baltimore, Johns Hopkins Univ. Press 1937), p. 55.

[2] *Marshall* v. *Barlow's Inc.* _____ U.S. _____ (19); Camara v. Municipal Court, 387 U.S. 523 (1967).

2. Presumption of Innocence

That brings me to a second principle of individual rights that is squarely at odds with computer-matching. Generally speaking, people in our society are not forced to bear a continuous burden of demonstrating to the government that they are innocent of wrongdoing. While citizens are obliged to obey the law--and violate it at their peril--presumption of innocence is intended to protect people against having to prove that they are free from guilt whenever the government chooses to investigate them.

There are many examples of how computer-matching can turn the presumption of innocence into a presumption of guilt. Later in my testimony I will cite examples of Massachusetts welfare recipients who have been summarily removed from the state welfare rolls as the result of a computer-match, and who are now fighting for reinstatement based on information the state neglected to take into account after their names appeared as "hits" in the match. A similarly striking example of this "presumption of guilt" occurred two years ago in Florida, when the state's attorney for a three-county area around Jacksonville obtained the case files for all food-stamp recipients in the area and then launched fraud investigations against those who had received allotments of more than $125 a month. A federal court of appeals invalidated the file search and enjoined the investigation on the ground that the targeted food stamp recipients were put in the position of having to prove that the allotment they had received was not based on fraud. Construing the Food Stamp Act, the Court held that "it did not allow the [state food stamp] agency to turn over files. . . for criminal investigation at any time without regard to whether a particular household has engaged in questionable behavior."[3/]

Once a computer-match has taken place, any person whose name appears as a "raw hit" by virtue of turning up on two unrelated computer tapes is presumed to be guilty of the wrongdoing under investigation--in part because the technology of computer-matching is so compelling and in part because its purpose--the detection of fraud and waste--is so commendable. The worst abuses of computer-matching, such as the summary termination of welfare benefits, have occurred when the government authorities conducting a match have casually transformed this "presumption" into a conclusive proof of guilt, based on no other evidence than a computer "hit".

3. Privacy Act

The most important principle governing the collection and use of personal information by the government is that the individual has a right to control information about himself and to prevent its use without his consent for purposes wholly unrelated to those for which it was collected. This principle is imperfectly embodied in the Privacy Act of 1974, 5 U.S.C. Section 552a, among whose flaws is that it has proved difficult to enforce.

[3/] Roberts v. Austin, 632 F.2d 1202, 1211 (5th Cir. 1980), cert. denied, 50 L.W. 3338 (1981) [emphasis supplied].

The Privacy Act restricts disclosure by federal agencies of personally identifiable information, such as the kind of information used in computer matches, unless the subject consents. There are two major exceptions to this rule. The first involves a "routine use," defined as "the use of [a] record for a purpose which is compatible with the purpose for which it was collected."[4/] The second involves a "law enforcement" disclosure, which enables an agency to be responsive to a request by another agency for information relevant to the investigation of a specific violation of law.[5/]

When computer matching was in its infancy at the federal level, the Privacy Act was correctly perceived by several federal agencies to be a major stumbling block for the new investigative procedure. The Civil Service Commission initially balked in 1977 at the plans of HEW Secretary Joseph Califano to institute a match of federal employee records and state welfare rolls, on the ground that the use of employee records for such a purpose would violate the Privacy Act. In a July 27, 1977 letter to HEW Inspector General Charles Ruff, the Commission's General Counsel, Carl F. Goodman, stated pointedly that the proposed match could not be considered a "routine use" of employee records, since the Commission's "information on employees was not collected with a view toward detecting welfare abuses." Similarly, it could not be considered a "law

---

[4/] 5 U.S.C. Section 552a(a)(7).

[5/] 5 U.S.C. Section 552a(b)(7).

enforcement" use, since "at the 'matching' stage there is no indication whatsoever that a violation or potential violation of law has occurred."[6/]

This candid and reasonable interpretation of the Privacy Act soon gave way to a succession of strained readings seeking to square computer-matching with the Act's prohibition on uses of personal records except for purposes compatible with the purposes for which they were collected.[7/] Since enforcement of the Privacy Act is left almost entirely to the agencies it regulates it is hardly surprising that the agencies have bent the Act to their own purposes and have now miraculously established that computer-matching is a "routine use" of personal records. All that is required to satisfy the policy of the Act, they say, is to publish each new computer matching "routine use" in the Federal Register

The Privacy Act has now been so thoroughly circumvented by executive action that it can no longer be seen as an effective safeguard against computer-matching abuses. Nevertheless, the principle underlying the Act that individuals should be able to exercise control over information about themselves which they provide to the government is a bedrock principle of individual privacy. That principle is at war with the practice of computer-matching.

[6/] Letter to Carl F. Goodman, General Counsel, U.S. Civil Service Commission, to Charles Ruff, Acting Deputy Inspector General, HEW, July 27, 1977, p.2, attached as Appendix A.

[7/] For a contemporaneous comment on this development, see Letter of John Shattuck to the Hon. Joseph A. Califano, Jr., December 8, 1977, attached as Appendix B.

4. Due Process of Law

Once a computer match has taken place it will result in a series of "hits," defined in the 1982 OMB guidelines as "the identification, through a matching program, of. . . specific individual(s)."[8] At this point all those identified are in jeopardy of being found to be guilty of wrongdoing. To the extent that they are not given notice of their situation and an adequate opportunity to contest the results of the match, they are denied due process of law.[9]

This is precisely what has happened in several of the best known matching programs conducted to date. For example, the results of Secretary Califano's Operation Match were kept secret from the federal employees whose records were matched with welfare rolls, because the Justice Department viewed the investigation "as a law enforcement program designed to detect suspected violations of various criminal statutes." Apparently for this reason the Justice Department ordered the Civil Service Commission not to notify any of the federal employees whose names showed up as "hits," since "[t]he premature discussion of a specific criminal matter with a tentative defendant is in our view inimical to the building of a solid prosecutorial case."[10] In Massachusetts the welfare authorities have gone one step further by terminating benefits of persons showing up as "hits" without even conducting an internal investigation of the validity and accuracy of the computer match results.

---

[8] 47 Federal Register, 21657 (may 19, 1982), § 4(f).

[9] See, e.g., Goldberg v. Kelly, 397 U.S. 254 (1970).

[10] Letter from Asst. Attorney General Benjamin R. Civiletti to Civil Service Commission Executive Director Raymond Jacobson, October 7. 1977.

This approach makes a mockery of both the legal and practical bases for due process of law. Due process is as old as Anglo-American jurisprudence. It is the right to confront one's accuser and introduce evidence to show that he is wrong. When the accuser is a computer tape containing information compiled from government records, the possibility of error is substantial. The practical as well as legal effect of keeping the subject of a "raw hit" in the dark about the results of a computer match is greatly to increase the likelihood that that an error will go undetected until it is too late to remedy without substantial cost to the individual as well as the government.

A travesty of due process can result from an agency's exclusive reliance on a computer match in determining whether to take action against the subject of a "hit". Following are several examples of erroneous welfare termination orders by the Massachusetts Department of Public Welfare, based upon a match of state welfare rolls with Massachusetts bank accounts. The examples are drawn from litigation challenging the match program currently pending in a Massachusetts federal court:[11/]

> Recipient, a resident of a nursing home, held a certificate of deposit in trust for a local funeral director, to be used for her funeral expenses. Her Medicaid was ordered

---

[11/] Lessard v. Spirito, Civil Action No. _____ (D.Mass. filed Nov. 5, 1982).

> terminated [when the computer match indicated that her bank account was above the Medicaid assets limit]. This decision is clearly wrong, because under federal regulations a burial contract account is an exempt resource.
>
> [The computer match showed recipient] to be $276 over the AFDC asset limit and her account was ordered terminated. Most of the money belonged to her brother who was in the army. She had previously disclosed this account to her social worker, who had told her not to worry about it.
>
> The recipient had a joint account with her 17 year old son, consisting of his money which he had received from his father and had earned. After the match [and after her benefits had been ordered terminated] the son withdrew a substantial amount of money (putting the account below the asset limit) in order to pay a debt to his grandfather. 12/

OMB Guidelines

Computer matching at the federal level has been regulated since 1979 by guidelines issued by the Office of Management and Budget. These guidelines, which were revised by the Reagan Administration in May 1982, are intended primarily to "help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching." 13/ In translation this means they are an effort to paper over the profound conflict between (1) the Privacy Act principle that personal records are to be used by federal agencies only for purposes compatible with those for which they were compiled and (2) the computer matching practice of joining personal record systems which have been compiled for wholly unrelated purposes.

12/ Affidavit of Allan G. Rodgers, Lessard v. Spirito, supra, at pp. 8-11, attached as Exhibit C.

13/ OMB Matching Guidelines, 47 Federal Register 21656 (May 19, 1982), §1.

To see how difficult and self-defeating the guideline-drafting task has been for OMB, it is necessary only to review the regulations issued by that office in 1975 when the Privacy Act was implemented. In these regulations OMB made very clear to federal agencies the major purpose of the Privacy Act: "One of the primary objectives of the Act is to restrict the use of information to the purposes for which it was collected."[14/] The parameters of this restriction are correctly described as "routine uses. . . that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public," such as agency "housekeeping measures."[15/] To make it plain that this was by no means an unlimited category, the regulations explicitly stated that "a 'routine use' must be not only compatible with, but related to the purpose for which the record is maintained."[16/] Finally, to nail the point down, OMB in 1975 pointed out that the statutory requirement that an agency give public notice of its routine uses of personal records was intended "to deter promiscuous use of this concept."[17/]

There is no way to reconcile OMB's interpretation of the Privacy Act with its guidelines on computer-matching. The 1979 guidelines represent an effort to work within the procedural

---

[14/] 40 Federal Register, 28953 (July 9, 1975) [emphasis supplied].

[15/] Id.

[16/] Id.

[17/] Id.

framework of the Privacy Act while circumventing its substantive requirements. The clearest example of this is the provision in the guidelines setting forth the steps that agencies must follow when planning computer matches of personal record systems which are, by definition, unrelated. The most important step is to publish a notice in the Federal Register defining the proposed match as a "routine use" of the records to be compared. Calling for the impossible, the guidelines make it even more difficult by requiring that "the notice should explain the justification of the routine use, including how the disclosure is compatible with the purpose for which the information [to be matched] was collected."[18] There is no way this requirement can be satisfied, since the matching of unrelated records will necessarily be unrelated to the purposes for which they were collected.

With this background, it is not difficult to see how OMB's matching guidelines have rendered meaningless the central principle of the Privacy Act. One example is enough to make the point. In 1980 the Office of Personnel Management published a notice in the Federal Register concerning its proposed use of personnel records for a matching program to help the Veterans' Administration verify the credentials of its hospital employees. The notice dutifully stated that the proposed match of OPM and VA records was a "routine use," which it explained as follows:

---

[18] 44 Federal Register, 23141 (April 18, 1979), § 5(c)(3)(a) [Emphasis added].

> "An integral part of the reason that these records are maintained is to protect the legitimate interests of the government and, therefore, such a disclosure is compatible with the purposes for maintaining these records." 19/

Under that broad justification any disclosure or matching of personal records would be permissible, since all federal records are purportedly maintained for the "legitimate interests of the government." If this is so, there is little basis for any claim that the OMB guidelines effectively, or even minimally, regulate the practice of computer matching.

Apart from this tortured effort to rationalize computer matching with the Privacy Act, the OMB guidelines do provide some restrictions on matching programs. These include requirements that only the minimum information necessary for a match should be disclosed, that there should be written interagency agreements on data use, that there should be controls on disposition and return of records, and that notices should be sent to OMB and to Congress concerning the creation of new systems of records as a result of any computer match. 20/

But this minimal list of protections is overshadowed by the fact that the guidelines contain no requirements or limitations on the conduct of computer matching in such critical areas as: (1) The nature of the record systems to be matched -- as far as one can discern there are no personal records, no matter how sensitive (e.g., medical files, security clearance records,

---

19/ Quoted in Kirchner, "A History of Computer Matching in the Federal Government," Computerworld, December 14, 1981, p. 15.

20/ 47 Federal Register, 2156-2158 (May 19, 1982) §§ 5a(2), 5b, 5d and 5e(2).

intelligence records, etc.), that are beyond the reach of computer-matching for any investigative purpose; (2) the procedures to be followed in determining the validity of "hits"--although the 1982 guidelines require agencies to publish "the procedures to be used in matching and following up on "hits,"[21/] no particular procedures are required to insure that the subjects of "hits" are afforded due process of law; (3) the standards and procedures to be followed for securing OMB approval of a proposed match--since the first set of guidelines was promulgated in 1979 OMB has not disapproved a single computer match, which is hardly surprising since it is not clear from the guidelines what role, if any, OMB is to play in reviewing the appropriateness of a proposed match; and (4) the projected costs and benefits of a proposed match, as well as the actual costs and benefits after it has been conducted--the 1982 guidelines have deleted all reference to cost-benefit analyses or reports on computer matches,[22/] thus apparently leaving it entirely to an agency's discretion whether to undertake a proposed match or to report its results in terms of costs incurred in running the program and benefits achieved in the recoupment of funds for the Treasury.

For all these reasons it is impossible not to conclude that computer-matching at the federal level is a huge unregulated

---

[21/] Id. § 5f(1)(b).

[22/] The 1979 guidelines had minimal requirements in this area. See 44 Federal Register 23139 (April 16, 1979), § 5a.

business, the only clear effect of which to date has been the undermining of individual privacy.

Examples of Computer Matches

There is no published compilation of computer matches conducted at every level of government, but it was recently estimated that more than 200 have occurred in the six years since the technique was first used.[23] At the federal level there have been matches for a wide variety of investigative purposes, using a broad range of personal record systems of varying degrees of sensitivity. These include matches of federal employee records maintained by the Civil Service Commission with files of persons receiving federal Aid to Families with Dependent Children, to investigate "fraud";[24] federal personnel records maintained by the Office of Personnel Management with the files of Veterans Administration hospital employees, to check "accreditation";[25] federal personnel records of Agriculture Department employees in Illinois with Illinois state files on licensed real estate brokers to "ascertain potential conflicts of interest";[26] IRS records of taxpayer addresses with lists of individuals born in 1963 supplied by the Selective Service System, to locate suspected violators of the

---

23/ New York Times, December 13, 1982, p. A1.

24/ The Washington Post, July 1, 1979, p. E3.

25/ Computerworld, December 14, 1981, p. 15.

26/ Privacy Times, June 9, 1982, p. 7.

draft registration law;[27/] and Labor Department files of persons entitled to receive Black Lung benefits with HHS records of Medicare billings, to investigate "double-billing medical fraud."[28/] These matches are only a handful of the total conducted, and even with respect to these, very little hard data is available, thanks in large part of the extraordinarily weak oversight and reporting requirements of the OMB guidelines, and the lack of attention to this subject by the Congress prior to the hearings of this Subcommittee.

I would like to review for the Subcommittee what little information is available on the public record about the conduct and results of several computer matches that have been conducted in recent years.

1. Project Match

Project Match was launched by HEW Secretary Joseph Califano in November 1977. It was aimed at comparing HEW employment records with welfare rolls in the Washington, D.C. area, and it was intended to be a pilot project for the eventual nation-wide match of five million federal employee records with welfare lists in twenty-six states. In September 1978 Secretary Califano announced the names of fifteen current or past agency employees who had been indicted on charges of welfare fraud based on the results of the match. None had been contacted when

---

[27/] Los Angeles Times, July 12, 1982, p. 1.

[28/] The Washington Post, February 18, 1982, p. A21.

their names showed up as "hits", although their names were released to the press when Califano made his announcement of the final results of the match.

The progress of the HEW trials was followed by the press. The following account by Evan Hendricks, editor of a respected Washington newsletter on privacy issues, was published in the Washington Post:

> Of the 15 HEW workers who were indicted--all of them welfare mothers--five had their cases dismissed, four had the charges reduced to misdemeanors, and the remaining six pled guilty to to felonies. None of those who had pled guilty had to serve prison time, and federal judges, unimpressed with the government's "best cases", ordered repayment of less than $2,000 29/

The overall data on the pilot project is similarly unimpressive. According to an October 26, 1978 status report, "the matching program resulted in 638 'raw' hits. The HEW Audit Agency determined that of these 'raw' hits, "480 were not worthy of further investigation because employment period or SSI payment period were not the same or because the file of SSI recipients contained those who had applied for SSI but who had not actually received payments. Of the original 'raw' hits, 158 cases were forwarded to the SSA Integrity Staff for further study. . . . Of the 158 cases referred, 41 are still under investigation for fraud and 55 fraud investigations have been closed with no further action to be taken. Also, 15 cases are still being investigated in the non-fraud area, while 45 have been closed." 30/

29/ The Washington Post, July 1, 1979, p. E3.

30/ Status Report on HEW Employment/SSI Recipient Project as of October 26, 1978, attached as Exhibit D.

Finally, to underscore the point that fraud did not appear to be the major problem in the administration of HEW public assistance programs, the same HEW office that conducted Project Match estimated that only 21% of the reported losses in the Aid for Dependent Children Program in 1977 were attributable to fraud.[31/]

2. Selective Service System-IRS

A very different but equally disturbing set of problems is posed by the matching of IRS taxpayer files with Selective Service lists of suspected non-draft registrants. Under this program IRS is using its computers to match addresses in IRS files with the names of 250,000 individuals supplied by the Selective Service System, all of whom will eventually receive notices in IRS envelopes that they face possible prosecution if they fail to register and that their addresses may soon be provided by IRS to Selective Service.

The issues raised by this match illustrate the danger of using the records of a particularly sensitive and unique agency, such as IRS, in any matching program, especially one with such a clear prosecutive purpose. First, the match involves IRS in a matter wholly unrelated to the enforcement of the tax laws, which depend in large measure on the willingness of taxpayers to provide large amounts of sensitive information about themselves. Second, the match raises the specter that the tax returns of those receiving the IRS letter will receive "special attention" because of

---

31/ The Washington Post, July 1, 1979, p. E3.

their suspected status as non-registrants. Third, the match seriously erodes taxpayers' confidence in the privacy of their tax records and the independence of IRS. All of these related dangers could have a devastating impact on the effectiveness of IRS as well as the rights of taxpayers.

If the IRS-Selective Service match is found to be an acceptable use of the computer-matching technique, there will be many agencies lining up outside the doors of IRS with similarly "compelling" proposals. As Representative Benjamin Rosenthal (D-NY), chairman of the House Subcommittee on Commerce, Consumer and Monetary Affairs, put it last summer in a letter to IRS Commissioner Roscoe Egger: "As you undoubtedly know, since the involvement of IRS in Watergate, the Service has resisted attempts by other Executive agencies to use it as a law enforcement agency for non-tax purposes. If IRS is to be used to secure compliance with the draft registration law, why should it not be used for compliance with the myriad other laws enforced by the Executive branch?"[32]

3. State Welfare Matches: Massachusetts and New York

At the state level computer match investigations of welfare fraud are also being conducted. Two large operations are underway in Massachusetts and New York. I will set out some recent developments in Massachusetts, and my colleague, Norma Rollins, will summarize the results of a report prepared by her Project on the costs and benefits of the New York program.[33]

32/ Letter of Rep. Benjamin Rosenthal (D-NY) to Hon. Roscoe Egger, Jr., Commissioner of Internal Revenue, July 21, 1982, p.2.

33/ Attached as Exhibit E.

The Massachusetts welfare-bank records match began in August 1982. The State Department of Public Welfare submitted computer tapes bearing the Social Security numbers of all welfare recipients in the state to 117 Massachusetts banks having a total of seven million deposit accounts. By comparing the Social Security numbers with bank account records the banks were able to identify for the state all welfare recipients who had cash assets beyond the allowable limit for persons on welfare. Upon receiving these lists of "hits" from the banks, the Department of Public Welfare did nothing further to check the accuracy of the assets information or to determine its relevance to the eligibility of particular recipients. Instead, it immediately sent out benefit termination notices to all those whose names appeared as hits.[34/]

The problems associated with this type of match are manifold. First, the use of bank account information raises many of the same far-reaching questions of confidentiality that are raised by matches involving tax records. A person's bank account is a mirror of his or her private life. Information from the account was never intended to be available to government investigators for the asking, as emphasized in the federal Right to Financial Privacy Act of 1978, which generally bars access to bank records except pursuant to legal process.

[34/] Plaintiffs' Memorandum in Support of their Motion for Temporary Restraining Order, pp. 2-3, Lessard v. Spirito, supra.

Second, the sending of termination notices to all welfare recipients showing up as "hits" on the welfare-bank match constitutes a denial of due process of law and a costly and inefficient method of managing the welfare system. As the pending litigation challenging the summary termination notices shows, there are many ways in which the "presumption of guilt" created by a "hit" on the match could be erroneous: the assets in an account may not be the property of the welfare recipient, the assets may be legally justifiable (e.g., to pay funeral expenses), the account may be held jointly by several people, etc.[35] In any event, the error rate for welfare terminations based solely on the fact of computer match "hits" appears to be exceptionally high, as shown by the fact that appeals of termination notices sent as a result of the computer match are being filed at *six times* the normal appeal rate.[36]

Third, and perhaps most important, the Massachusetts program demonstrates how utterly ineffective a computer match is in providing the kind of detailed, variable and verified information that is needed to reach a conclusive judgment about whether a person is eligible for welfare or has committed welfare fraud. For example, each welfare program exempts certain types of assets in determining eligibility. Beyond certain very basic items like the home in which the welfare recipients reside, the specifics of these exemptions vary greatly from program to program. Although the streamlining of eligibility requirements would certainly serve to improve the management of most welfare programs, the current complexity of these requirements renders both meaningless and dangerous the kind of simplistic "hit" information provided by the Massachusetts welfare-bank account match.

---

[35] Affidavit of Allan Rodgers, attached as Exhibit B.

[36] Plaintiffs' Memorandum, *Lessard* v. *Spirito*, *supra*, p. 5.

Recommendations and Conclusion

Computer-matching is an attractive investigative technique. It appears to permit law enforcement officials for the first time instantaneously to root out all instances of a particular kind of wrongdoing in a particular segment of the population. It constitutes a general surveillance system which supposedly can detect and deter misconduct wherever it is used. It appeals to the view that "if you haven't done anything wrong, you don't have anything to worry about."

But there are heavy costs associated with computer-matching, both in terms of individual rights and in terms of law enforcement expenditure, and it is not at all clear that the benefits of the technique outweigh the costs.

Upon close examination computer-matching has been hard pressed to line up to its advanced billing. The comparison of unrelated record systems is fraught with difficulty. Data on the computer tapes may be inaccurate, or inaccurately recorded. It may present an incomplete picture of the persons to whom it pertains. It is unlikely to be sufficient to "answer" difficult questions, such as whether a person is entitled to receive welfare or is engaged in a conflict of interest. On the other hand, computer-matching most certainly erodes a wide variety of individual rights, such as the Fourth Amendmnet right to be free from unreasonable search, the presumption of innocence, the right to due process of law and the right to limit the government's use of personal information to the purposes for which it was collected. Moreover, the rapid and unchecked growth of computer-matching leads inexorably to the creation of a de facto to National Data System in which personal data is widely and routinely shared at all levels of government and in the private sector.

The hearings of this Subcommittee are a welcome opportunity, long overdue, to look closely at computer-matching before it grows beyond control. As a general framework for the development of safeguards of individual rights, I propose the following:

1. The Privacy Act should be amended to clarify that computer matches arenot ipso facto, "routine uses" of personal record systems.

2. No further federal computer mathces should be permitted without express congressional authorization.

3. Congress should not authorize computer matches of sensitive personal records sytems, the confidentiality of which is otherwise protected by statute, such as taxpayer records maintained by the Internal Revenue Service, census records maintained by the Census Bureau, or bank records maintained by federally insured banking institutions.

4. No computer match should be authorized unless and until an analysis has been made of its projected costs and projected savings in the recoupment of funds owed to the government, and a determination has been made that the public benefit will far outweigh the cost and that individual rights will be protected. The results and full costs of any match that is undertaken should be published.

5. Procedural due process protections for the persons whose records are to be matched should be specified by statute, including the right to counsel, the right to a full hearing, and the right to confidentiality of the results of a match.

These are only tentative and preliminary recommendations. Needless to say, the entire thrust of my testimony has been to raise profound questions about the development of computer-matching. The thrust of my recommendations is the call for a moratorium on all further matching to give the Congress and the public an opportunity to study the results of all the computer-matching programs that have been conducted to date and the long-term consequences of further developing this technique. In the end, I must agree with Justice Douglas that "I am not ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals."[32/]

Thank you for the opportunity to appear before the Subcommittee.

[32/] California Bankers Association v. Shultz, ____ U.S. ____ (1973) (dissenting).

APPENDIX A

UNITED STATES CIVIL SERVICE COMMISSION
WASHINGTON, D.C. 20415

IN REPLY PLEASE REFER TO
GC:LEG 1
LF:kab

YOUR REFERENCE

JUL 27 1977

Charles Ruff, Esq.
Acting Deputy Inspector General
Department of Health, Education and
  Welfare
Room 5262, North Building
4th & Independence Avenue, S.W.
Washington, D. C. 20201

Dear Mr. Ruff:

As you know from meetings with staff of this office, we have expressed concern about the compatibility of "Project Match" with the restrictions placed on agencies by the Privacy Act of 1974 (5 U.S.C. § 552a). The project would furnish computer files of the Commission containing the name, date of birth, social security number, salary, and duty location to your office for comparison with State welfare rolls to detect abuses in the Aid to Families of Dependent Children (AFDC) program.

The legislation creating your office (42 U.S.C. § 3521) provides, in pertinent part, that agencies shall furnish information when to do so would not contravene existing statutory restrictions or agency regulations and:

> "(3) In the event any record or other information requested by the Inspector General. . .is not considered to be available under the provisions of section 552a(b)(1), (3), or (7) of title 5, United States Code, such record or information shall be available to the Inspector General in the same manner and to the same extent it would be available to the Comptroller General."

The information to be furnished would be obtained from the Commission's Central Processing Data File (CPDF). Because the information therein is within the definition of "system of records" at 5 U.S.C. § 552a(a)(5), the restrictions imposed on disclosure by the Privacy Act without the written consent of the individuals to whom the information pertains, would be applicable.

THE MERIT SYSTEM—A GOOD INVESTMENT IN GOOD GOVERNMENT

Although the quoted portion of the statute refers to availability under 5 U.S.C. § 552a(b)(1), (3), (7) and to the same extent the information would be available to the Comptroller General, we have some doubts that any of these provisions are clearly applicable to permit disclosure under the circumstances presented here.

At 5 U.S.C. § 552a(b)(1) disclosure is permitted where it would be "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.". Since this would be an inter-agency rather than an intra-agency disclosure, (b)(1) is patently inapplicable.

Disclosure is permitted under (b)(3) for a "routine use" established by the agency. Among the routine uses established by the Commission for its "CSC/GOVT-3" system of records at 41 Fed. Reg. 42164 (Sept. 24, 1976) is the following:

> "p. Disclosed to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order where there is an indication of a violation or potential violation of civil or criminal law or regulation."

The difficulty with disclosure under the routine use provision is two-fold. At subsection (a)(7) of the Act, "routine use" is defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected". Although the literal terms of this provision obviously cannot be followed with precision in practical application to agency operations, it is evident that this information on employees was not collected with a view toward detecting welfare abuses. Secondly, and perhaps more significantly, at the "matching" stage there is no indication whatsoever that a violation or potential violation of law has occurred. It is only after a comparison of data between those currently on Federal payrolls and AFDC rolls produces a "match" that a possible or potential violation of law warranting further inquiry is evident. It cannot fairly be said, therefore, that disclosure of information about a particular individual at this preliminary stage is justified by any degree of probability that a violation or potential violation of law has occurred.

It has been suggested that (b)(7) would permit disclosure under these circumstances. That provision sanctions disclosure "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought."

While this provision seemingly eschews the requirement of the routine use quoted above that there must be some indication of a violation or potential violation of law before disclosure is sanctioned, its emphasis on specificity suggests that it was not intended to permit broadly-worded, all inclusive requests either for all the records on a given individual or certain information on a large class of persons. Indeed, the Office of Management and Budget in its guidelines interpreting the Act warns, "(b)lanket requests for all records pertaining to an individual are not permitted". 40 Fed. Reg. 28955 (July 9, 1975). A reasonable corollary of this provision would be that blanket requests for certain information on a broad category of individuals are not permitted.

The enabling legislation creating the Inspector General's office, in addition, permits disclosure "in the same manner and to the extent [the information] would be available to the Comptroller General." It is difficult, however, to conceive of a situation where the Comptroller General in carrying out his audit-investigative functions could properly make the sort of broad request at issue here for the purpose of matching records to determine whether violations of law have occurred. We recently expressed our reservations to the General Accounting Office concerning a proposal whereby agencies would furnish the Commission with a list of individuals against whom Federal agencies have a claim for unpaid debts to match against records of current and retired Federal employees for the ultimate purpose of assisting agencies in debt collection. A copy of our comments to the General Accounting Office is attached.

Notwithstanding the above, we believe an argument can be made that subsection (b)(2) of the Act sanctions disclosure under these circumstances That provision permits disclosure where it would be required by the Freedom of Information Act. Admittedly, it is not clear that Congress contemplated one agency would use the FOIA as the basis for requesting agency records from another. On the other hand, agencies have received a multitude of requests for records from members of Congress under the Act and it seems no more inappropriate for an agency to use the Act as a basis for disclosure of records to another agency than for Congress to use it in a similar fashion.

The use of the FOIA as a basis for disclosure requires consideration of exemption (6) and whether or not the invasion of personal privacy that would ensue from disclosure of the information involved in this program would be outweighed by the public interest served thereby. The only items of information involved here that are not considered in the nature of public information as prescribed by Commission regulations at 5 CFR § 294.702 would be employee social security numbers and dates of birth.

That there would be a substantial public interest served by the disclosure is clear from the nature of the proposed program. It has been estimated that the program would result in a potential savings of $10,000 for every identified case of abuse. The statutory scheme establishing the Office of Inspector General itself suggests the public benefit that would be served by its operations. Finally, the reported discussion of Project Match in a Cabinet-level meeting reflects a determination at the highest Executive Branch level that this projected program promises to yield dividends for the general public in terms of tax dollar savings.

When the public interest to be served is balanced against the minimal invasion of personal privacy that would occur, it seems clear that the former would predominate and require disclosure under the FOIA thus permitting disclosure under (b)(2) of the Privacy Act. We understand that this is the substance of the approach discussed with you as the basis for our cooperation in a recent meeting involving the Executive Director of the Commission and the Deputy General Counsel.

Apparently, the Departments of Agriculture and Labor are interested in similar initiatives to detect abuses found in programs for which they are responsible. Since we are not aware of legislation similar to that creating your office which at least suggests disclosure of information may be permitted notwithstanding the restrictions contained in the Privacy Act, we would feel a greater reluctance to furnish information for matching purposes to those agencies. Because the Commission will apparently be faced with additional requests from other agencies in the future, perhaps the best solution for determining the legality of providing this type of information to agencies in general for "match-type" projects would be to seek guidance from the Justice Department. If we can assist you in this regard, please let us know.

Sincerely yours,

Joyce L Evans
Carl F. Goodman for.
General Counsel

Attachment

APPENDIX B

December 8, 1977

The Hon. Joseph A. Califano, Jr.
Secretary
Department of Health, Education
and Welfare
Washington, D.C.

Dear Mr. Secretary:

In its commendable desire to eliminate welfare abuse, the Department of HEW has failed to consider the serious threat to privacy posed by its computer search operation known as Project Match, which you announced in your press conference of November 9.

We understand that Project Match is intended to permit a general search of the personnel records of government employees for evidence of welfare fraud. The assumption within the Department seems to be that the benign purpose of Project Match insulates it from criticism based on privacy concerns. The fact that this particular computer use is designed to eliminate welfare fraud, however, does not in any way lessen the massive threat it poses to individual privacy. Indeed, this very type of search operation was highlighted in the Privacy Protection Study Commission's recently released report, Technology and Privacy. The Report noted that "the ability to search through hundreds of thousands, or even millions, of records to identify individuals with particular characteristics of interest is at once the most important gain, and the most important source of potential harm, stemming from the automation of large-scale personal data record keeping systems, . . ." [emphasis added].

While much of the literature on technology and privacy points up the need for new laws to protect privacy rights, the implementation of Project Match is particularly disturbing because it violates the spirit, if not the letter, of existing law. The Privacy Act of 1974 restricts the disclosure by federal agencies of personally identifiable information unless the subject has consented. Although the release to HEW of payroll records for the purpose of identifying welfare recipients does not appear to have been within Congress' intent when it enacted certain exemptions to the Privacy Act's general prohibition, the Department obtained a computerized military payroll under the "routine use" exception to the Act.

When the Department approached the Civil Service Commission to obtain access to the master tape of federal civilian employees, the Commission determined that disclosure of the information would violate the Privacy Act. The Commission nevertheless released the information to the Department, citing the Freedom of Information Act in support of its decision. A federal agency, however, is not a person within the meaning of the FOIA and therefore cannot gain access to records under the Act.

We believe that Project Match, whether or not it is technically in violation of the Privacy Act or the Freedom of Information Act, is precisely the kind of data-matching operation that the Privacy Act was meant to prevent. Certainly, the examination of a list of fedezal employees against a list of welfare recipients is incompatible with the purpose for which either of those record systems was originally compiled. HEW itself, in the 1973 Report of its Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, identified as one of the cardinal principles of a code of fair information practices that personal data obtained for one purpose must not be used *or made available* for other purposes without the individual's consent.

Project Match exemplifies precisely the kind of manipulation of personal data that people most fear when they contemplate the vulnerability of their privacy in a computer age. The demonstration of public concern in recent years over the proliferation of uses of the Social Security Number and its de facto transformation into a universal identifier is testimonial to a growing awareness of the ease with which separate data systems can be brought together for comparison and amalgamation. If the government can now match federal and even private payrolls against the welfare rolls, why should it not, as some future time, match the federal payroll against computerized lists of medical and other social services beneficiaries, or against computerizes lists of contributions to political parties, or ggainst computerized indexes of police intelligence records? In each of these instances, a case could be made for the usefulness of the resulting "hits," in terms of administrative efficiency or law enforcement or any of a number of socially desirable ends. The same techniques and justifications could readily be used to search for social or political "deviants" as are now being used to search for welfare "cheaters."

We must also take exception to the argument that Project Match is acceptable because its ultimate end is law enforcement. We cannot think of any better example of a constitutionally proscribed general search than a random rummaging through the contents of massive records systems on the chance that "something will turn up." Here, people become the targets of a search merely because they are members of a category--government employees or welfare recipients. Project Match is intentionally designed as a general search, since there is apparently no evidence to direct suspicion of fraud to any particular member of these groups; it is a classic fishing expedition.

The danger of Project Match is that its goal, to expose and control welfare fraud, is one of which everyone canaapprove. But in light of HEW's own historical leadership in defining issues of individual privacy raised by the data-keeping practices of governmental agencies, we would expect HEW to be more sensitive to the long-range implications of an operation such as Project Match.

We urge you to reconsider the Departmentâs approach to the detection of welfare fraud and to devèlop methods of investigation less damaging to privacy and civil liberties than Pøoject Match.

Yours sincerely,

John H.F. Shattuck
Director

APPENDIX C

Exhibit A

AFFIDAVIT OF ALLAN G. RODGERS

I, Allan G. Rodgers, on oath depose and say:

1) I am an attorney and director of the Massachusetts Law Reform Institute, a program that provides legal services to poor people and support to persons in other legal services programs in the state. On October 14, 1982, I and several of my colleagues met with Henry Cretella, General Counsel, Joseph Gallant, Assistant to the Commissioner and Fred Brown of the Commissioner's Control Center, all employees of the Department of Public Welfare. All three had been working on, or were involved in meetings about, the Department's bank account computer matches. The information set forth in paragraphs 2-9 of this affidavit is taken from what one or more of these three persons told us at that meeting.

2) In August of this year the Department started to match by computer the social security numbers of all members of the assistance units of all six assistance programs operated by it (Aid to Families With Dependent Children - AFDC; General Relief - GR; Food Stamps; Medicaid; Supplemental Security Income - SSI; and the Refugee Resettlement Program - RRP) with the social security numbers of account holders in certain banks in the state. These matches have been completed in phases as banks have

agreed to them. To mid-October, four matches had been done with a total of about 10% of the state's some 1,000 banking institutions. These four phases matched only social security numbers, not names or other identifiers. It appears that the Department furnished its own tapes to each bank, which matched the tapes with its own tapes and sent the matches back to DPW for further screening.

3) Upon receiving the raw information from the matches with the banks, the Department eliminated from consideration those cases where the amount in the accounts did not exceed the asset limit for each assistance program in which the individual's assistance unit was participating. It also screened out cases where the account was within $500 of the assets limit ($250 for GR individuals) and referred those cases to the local welfare services offices for further checking, but see ¶15, infra. It then issued immediate termination notices to those remaining "hits." As of October 13, 1982, 1,621 termination notices had been mailed to recipients of all programs except SSI. SSI cases were referred to the Social Security Administration, which has chosen to investigate cases Before taking action on them.

4) Contrary to prior DPW practices, including practices on wage matches, the termination notices were not sent from the local welfare offices but centrally from the Commissioner's Control Center (CCC) in Boston. Prior to sending the notices, the Department did not contact the banks to inquire about whether the names of those to be terminated were on the accounts or whether there were any errors in the social security numbers at

the banks or at DPW. Neither did the Department first review the recipients' case files to see whether there was a satisfactory explanation of the bank account or a record that the recipient had previously reported the account. Nor did the Department undertake any redetermination of current eligibility. The Department did not initially send any information on the bank accounts or the terminations to local offices, with which recipients are used to dealing, but the termination notices instruct recipients to contact persons at the CCC in Boston. The termination notice itself, a copy of the computer printout showing the bank account and any other information collected by the CCC are sent to the Department's representative at hearings (usually the assistant director of the community service area). No instructions have been given as to whether or not these papers are placed in the recipients' case file nor as to when and how they may be made available in the local welfare service office to the recipient or her representative prior to the hearing, and DPW central office people do not know what the local office practices are.

5) All persons sent termination notices have had their cases referred to the Bureau of Special Investigations for a fraud investigation. Recipients are not specifically notified of a BSI referral. There are no written instructions on whether a copy of the fraud referral form is usually placed in the recipient's case file, and DPW central office people do not know what the local office practices are.

6) As of mid-Octobver, 30% of the persons receiving

termination notices had appealed for a fair hearing to challenge their terminations. This is six times the usual appeal rate of 5%. Of those who have appealed, the Department says that half involve errors in social security numbers. This is an error rate of 15% of all those who were sent termination notices. Most of the errors have occurred because bank records contained incorrect social security numbers.

7) The Department, through its attorney staff, has adopted a policy of filing civil court actions against recipients to recover alleged overpayments of assistance as a result of undisclosed excess assets, and to secure ex parte attachments of the bank accounts revealed by the computer matches. As of mid-October, the Department had filed some 100 of those actions.

8) The Department plans to continue the computer matches, as banks agree, until all banks in the state are included. It may do future matches by using the first two letters of each person's last name as well as social security numbers.

9) The Department did not request or receive from the federal government any approval or waiver to conduct these computer matches, except that it requested from the Department of Health and Human Services a waiver of application of error rate fiscal penalty standards to the undisclosed assets uncovered by the computer matches.

10) On September 10, 1982, the Department filed with the Massachusetts Secretary of State a purported emergency regulation, State Leter 607, regarding undisclosed assets and

rules governing bank accounts of recipients in the AFDC program. Attached as Appendix A is a copy of the page which I obtained from the Secretary of State's Office, containing the Department's statement of the emergency which claims to have justified making the regulation effective without going through the notice and comment requirements of the state's Administrative Procedures Act. Henry Cretella, the Department's General Counsel, told me on October 18 that the Department was rethinking S.L. 607 and might well make some changes in it.

11) Since our office is a state support center for all legal services programs that represent poor people in the state, we have been in constant touch with lawyers and advocates across the state who have been approached by recipients who have received termination notices as a result of the bank account matches. We have made a survey of these programs and count 101 families, of the 1,621 who received termination notices as of mid-October, who are being represented by legal services programs, which are virtually the only source of legal assistance for these recipients. This represents only 21% of those who have requested fair hearings on their terminations. In additioin, 24 (or nearly 25%) are pure errors, and most of the rest are cases where the recipient clearly does not own or have access to the account.

12) At the request of the Department of Public Welfare, our office secured copies, with names of recipients erased, of 23 fair hearing decisions on bank account match terminations. These were said by Department representatives to be the only decisions available on this topic at the time we obtained them on October

26. I personally have reviewed these decisions. Copies are available upon request, and I have numbered them 1-23. Of the 23 decisions, 10 resulted in favorable decisions for the welfare recipients. Of these 10 favorable decisions, 5 represented pure errors in social security numbers (2 of which were the errors of the Welfare Department) which could have been corrected by communicating with the bank (#1,2,3,4, and 21). Five other recipients won their appeals at the hearings. Four of these wins involved the withdrawal by recipients of funds so that at the time of the notice of termination, or at the time of the hearing, the amount remaining in the account was below the applicable asset limit. (#5,6,8 and 9). In only one of these cases was the recipient able to prevail on the argument that no one in the assistance unit had access to the bank account (the account was in the name of the separated father for a son who was in the assistance unit - #7).

13) The Department's practice is to list the name of a representative who appeared at the hearing for the recipient, on the lower left of the last page of the decision. Of all the recipients who appeared at the hearings in these cases, none was apparently represented by a lawyer or by an experienced advocate. One recipient was represented by a social worker at the nursing home in which she resided (#16). Two others apparently had friends or neighbors assist them (#2,8). All other recipients were unrepresented at these hearings.

14) Three recipients who appealed for a fair hearing had their benefits terminated, prior to the hearing, despite their

having filed a timely appeal, in apparent violation of law (#3,18 and 21). In two of these cases, the recipient prevailed at the hearing (#3 and 21).

15) Despite the Department's claim that it was not terminating recipients where the computer match showed a bank account within $500 of the asset limit ($250 for GR)(see #3 of this Affidavit), these decisions show seven cases where termination notices were sent even though the alleged assets were within the tolerances (#5,8,11,13,19,20 and 21). In three of these cases, the appellant won (#5,8 and 21). In one case, the AFDC family was terminated for being $26 over the asset limit (#20).

16) In five of the cases, the recipient's benefits were ordered terminated by the referee as of the date of the hearing rather than later as per the termination notice (#14, 15, 17,19 and 22).

17) So far as appears from the hearing decisions, the only evidence presented by the DPW representatives was the results of the computer match itself. In each case, therefore, apparently the recipient had the burden of coming forward with evidence to disprove the computer match information.

18) There are many inconsistencies among these decisions on what rules should be applied as to the timing of counting the assets as being in excess of the asset limits. In four cases (see §12 above) the recipient won the hearing because of a later spend-down on the account below the asset limit, despite the fact that the computer match showed that the recipient had earlier

been over-asset. In six other cases the recipient lost the hearing despite the fact that the the account was below the asset limit on the date of the termination notice or on the date of the hearing (#10,11,12,17,18 and 19). These decisions thus do not reveal any consistent rules that are applied to this issue.

19) In 13 of the cases, the recipient's appeal was denied. In nearly all of these decisions, it is my judgment that the hearing decision is either wrong on its facts, or is seriously open to question on factual or legal grounds. A summary of these hearing decisions follows:

(a) The recipient had a joint account with her 17 year old son, consisting of his money which he had received from his father and had earned. After the match and before the hearing, the son withdrew a substantial amount of money (putting the account below the asset limit) in order to pay a debt to his grandfather (#10).

(b) This recipient was alleged to be $276 over the AFDC asset limit. She testified that most of the money belonged to her brother who was in the army in Germany. She had previously disclosed this account to her social worker, who had told her not to worry about it. Some money was withdrawn and sent to the brother prior to the date of the hearing, leaving the account below the asset limit (#11).

(c) The recipient had admitted "that the bank accounts are hers, an account with her daughter and her daughter's account with her father." It was held that since the recipient and her dependents had access to the accounts, they were attributable to the assistance unit. The facts set forth in the opinion do not indicate whether her daughter is a minor and are otherwise too skimpy to enable one to tell whether the decision is correct (#12).

(d) This General Relief recipient had a $500 bank account jointly with her sister, and said that the money belonged to her sister. Prior to the termination notice, the account was changed and put in her sister's name in trust for the recipient (#13).

(e) The recipient held a joint account with her daughter, of which she testified she owned less than the asset limit (#14).

(f) Recipient mother and her son held a joint account, consisting of money left to her son by will (#15).

(g) Recipient, a resident of a nursing home, held a certificate of deposit in trust for a local funeral director, to be used for her funeral expenses. Her Medicaid was ordered terminated (#16). This decision is clearly wrong, because under federal regulations a burial contract amount is an exempt resource. See 42 CFR §§435.322 and 435.845(d); 20 CFR §416.1201(a)(2)

(h) Recipient held a term deposit and stated she was not aware of the resource limits. Prior to the hearing, she withdrew the money and said she intended to use it to prepay funeral expenses for herself and her two children (#17).

(i) Recipient said that money in an account held jointly in the name of herself and her son belonged to her son, who was in the service. Two days before the notice of termination, she withdrew enough to leave the account below the asset limit. Three days after the termination notice, she withdrew the balance and sent it to her son. The referee held that she could reapply for GR because she no longer had the asset, but stated that she was ineligible for food stamps, because she had an account exceeding $1500 as of the termination notice date. This is clearly wrong, because according to the facts cited in the referee's decision, her account contained $1,110 as of the termination notice, which is below the $1500 asset limit for the food stamps program (#18).

(j) Recipient held a bank account jointly between herself and her two sons, which was $177.99 over the AFDC asset limit on June 30, 1982. She subsequently withdrew $600, so that she had $577.99 on the date of the notice of termination. She also stated that she had tried to report the account to her social worker but it was not listed by her worker because she said the money belonged to her sons (#19).

(k) This AFDC recipient held five bank accounts, totalling $1,026 as of the date of the computer match, in trust for each of her five children. She said the money was given to her children by their grandmother to be used for the education of her children. There had been no activity on the accounts since 1979. The referee ordered her assistance terminated, but requested the Department to allow her to reduce her account below the $1,000 asset limit and to reapply. The referee also asked the Department to forego recoupment (#20).

(l) Recipient had one account of slightly below $2,000 in her own name. In her GR application filed on April 27, 1982, she declared she had no assets because she thought she could have $2,000 in the bank. She also held a second account jointly with her mother, who was a nursing home resident, which she claimed belonged to her mother (#22).

(m) Recipient held a $20000 term deposit certificate and a $6,887 savings account each in trust for her mother, whom she showed inherited that money. In 1977 she disclosed these to her social worker, and no action was taken. The daughter had not withdrawn any of the money sinces she received it (#23)(see affidavit of Joan Black - Ex. I).

Signed under the pains and penalties of perjury this 3rd day of November, 1982.

Allan G. Rodgers

APPENDIX D

STATUS REPORT ON HEW EMPLOYEE/SSI RECIPIENT PILOT PROJECT AS OF OCTOBER 26, 1978

The data on the pilot matching program between SSI recipients and HEW employees is not yet complete. We are currently in the process of requesting detailed reports from the SSA District Offices on numbers of overpayments and numbers of ineligibles found as a result of the matching program.

The matching program resulted in 638 "raw" hits. The HEW Audit Agency determined that of these "raw" hits, 480 were not worthy of further investigation because employment period and SSI payment period were not the same or because the file of SSI recipients contained those who had applied for SSI but who had not actually received payments. Of the original "raw" hits, 158 cases were forwarded to the SSA Integrity Staff for further study.

The breakdown of the 158 cases is shown on the enclosed chart. Of the 158 cases referred, the report shows that 41 cases are still under investigation for fraud and 55 fraud investigations have been closed with no further action to be taken. Also, 15 cases are still being investigated in the non-fraud area while 45 have been closed. Two cases have been referred for prosecution as of October 26, 1978, one in New York and one in Philadelphia. The cases listed under non-fraud in the District Offices reflect cases with problems in the social security numbers which are being resolved by those offices.

OIG/HCSR/JAllen/kdg/11/3/78

FILE COPY

OFFICE	SURNAME	DATE	OFFICE	SURNAME	DATE	OFFICE	SURNAME	DATE

PRIVACY
JOURNAL

P.O. Box 8844
Washington, D.C. 20003
(202) 547-2865

an independent monthly on privacy in a computer age

ROBERT ELLIS SMITH
Publisher

Statement of Robert Ellis Smith

Publisher, PRIVACY JOURNAL

Washington, D.C.

at

hearings on computer matching

Before the Senate Committee on Governmental Affairs

Subcommittee on Oversight of Government Management

December 16, 1982

Less than a decade ago, the Congress declared as a matter of public policy that exchanges of personal information among federal agencies and from federal agencies to others ought to be discouraged. It enacted the Privacy Act of 1974, which prohibited such exchanges except in certain circumstances. Three years after that, the Department of Health, Education and Welfare, under its secretary, Joseph A. Califano Jr., launched a highly publicized "Project Match" to run computerized welfare lists against payrolls and other lists to identify which persons might appear on both lists and therefore possibly be collecting public assistance in violation of eligibility requirements.

Even though the dollar amounts lost through fraud and waste are probably greater involving persons in the middle and upper levels of our society, HEW chose to prey on the most vulnerable of all recipients of government assistance, welfare recipients. Only after this had occurred, in March 1979, did the Office of Management and Budget, which was designated by Congress to oversee compliance with the Privacy Act, issue guidelines for federal computer matching programs. The guidelines essentially ratified what HEW had initiated, but they did establish certain paperwork procedures that required federal agencies to think twice before conducting matches. In May 1982, the OMB repealed even those slight safeguards.

Now, five years after Califano's project, this hearing marks the first time that public policymakers have stopped to consider whether these computer matches are effective, are fair, are an invasion of personal privacy, and are in the best interests of the public. As the publisher of a monthly newsletter on the right to privacy and a person who has researched the conduct and effect of these matching projects, I believe that the public is not at all getting its money's worth from these schemes and, more important, computer matching violates the letter and the spirit of the Privacy Act of 1974 and invades individual privacy. The victims of these invasions of privacy are the most vulnerable members of our society -- poor people -- because their representation in the halls of power is the weakest. (A poll by Louis Harris in 1979 showed that 98 percent of business executives and 87 percent of the public approved of these welfare matches; but slightly more than 50 percent of business executives and 68 percent of the public approved of identical matches to compare credit card records with tax returns to catch tax evaders. (1) I'm confident that when fully informed of computer matching, most of the public will disapprove.)

Now comes the coordinator of the government's matching programs, Richard P. Kusserow of the Department of Health and Human Services, to say that computer matching ought rightly be called "an editing function." Matches do no more than "cleanse data bases," for efficiency and economy, Kusserow told his colleagues last month. This brings to mind George Orwell's 1984, not because of the pervasive surveillance portrayed in that novel but because of its invention of a new language, Newspeak, with a vocabulary of deceptive euphemisms intended to pacify the populace. In Orwell's 1984 peace meant war; in America's 1984 "an editing function" means knocking people off welfare. (2)

The Victims

Consider the "editing function" by HEW in the late 1970s: After claims that it would save millions of dollars, the general search of federal payrolls turned up 15 current or past HEW employees who were indicted on charges of accepting public assistance while simultaneously holding a job. In the end less than $2000 was paid back to the government by all those involved, but the process was a painful one for the 15 mothers involved, none of whom was notified before Califano announced the indictments.

One woman had quit nursing school and accepted welfare when told she had cervical cancer. After months of cobalt treatment, she convinced her doctor to let her go back to work. She found a job with an HEW agency, and twice she notified the welfare department. As often happens in these cases, a social worker told the woman not to worry if she received a few more checks. But the checks kept coming for some time, and after a while the woman could not resist the temptation to cash them to pay her doctor's bills. After the computer match was conducted, she was called from her job and interrogated by three department investigators. She tried to explain the situation, but the investigators would only tell her that Califano wanted to put an end to welfare cheating.

She was so shaken by the confrontation that she quit her job. Three months later, friends called her to tell her that her name was in the paper as a welfare cheat. She and her children obviously were shaken by this. Kusserow's "editing function" for a welfare mother is the equivalent of a doctor telling a patient that he has cancer and should return to the office in a month for more details.

The woman was told to plead guilty by her court-appointed attorney, and she was about to do so when the judge asked her whether she had notified the welfare agency that she had taken a job. When she replied that she had, the judge threw the case out of court, but not before there had been a major disruption in the life of the woman and her children. (3)

Inaccuracies

This case illustrates an accurate match. There are thousands of inaccurate matches, because even the best laid data-processing plans go astray. At a meeting last November of the Association of Access Professionals, speakers from the Department of Health and Human Services and the Veterans Administration stressed how many things can go wrong -- and do -- in computer matches. Most of the "hits" are invalid because there is a mistake in Social Security numbers or names or, as in Massachusetts, welfare lists of one month are compared to employer lists of several months earlier or because there is a valid explanation for a person appearing on both lists. (Federal agencies have many low-paying jobs and internships that would not disqualify a person for public assistance.) The Veterans Administration thought it caught 1500 persons receiving regular checks who also appeared on a Social Security computer list of persons known to be dead. In fact, the 1500 were widows of deceased veterans who were using their husbands' Social Security numbers with the VA because they thought that was proper. (4)

The Veterans Administration representative, James Durnil, pointed out that a lot of data collected by a particular agency is not crucial to that agency and so it is never checked for accuracy (one's date of birth on an application for a farm loan, for instance). When that information becomes the basis for a match with a second agency, that inaccurate information takes on crucial importance. Durnil is aware of this phenomenon, but his agency continues to conduct matches at the rate of five a week.

Misinterpretations

This is exactly what Sen. Sam Ervin wanted to prevent when he co-sponsored the Privacy Act in 1974. In the debate on the "routine use" exception, Sen. Ervin said in the Senate, "This act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." (5)

There is a perfect example of this in Massachusetts, where the state government is demanding to match welfare lists against the bank's lists of the names, Social Security numbers, and current balances of its customers. About 15 percent of the Social Security numbers are found to be inaccurate because banks merely collect the numbers from customers because the Internal Revenue Service requires them to do so. The banks do not use the number, nor do they care about its accuracy. (6)

But in Massachusetts, on the basis of these erroneous hits, the head of a family receives a notice of assistance termination. This shifts the burden to the recipient to prove at a hearing (rarely represented by an attorney because Legal Services have been severely cut back) that he or she is not in violation.

A typical welfare recipient might receive a check for say $700 from an insurance claim or an inheritance, deposit it in the bank and then immediately pay bills by check. If Kusserow's "editing function" occurs on the wrong day, the recipient is terminated from public assistance. Most of the "hits" of bank records in Massachusetts show a bank balance of $500 to $1000 more than the permissible ceiling on cash assets. (7)

Or take the case of an elderly woman who, nearing her death, agrees to add her daughter's name to a joint bank account holding the meager cash of the mother. It is clear to everybody that the money in the bank still belongs to the mother, but the daughter's name has been added to the account so that she may have ready access to it when the older woman dies. This is poor people's estate planning, according to a Boston attorney defending the victims of computer matches. The Social Security number of the daughter, a welfare recipient, shows up on the computer match and she is terminated from public assistance, because she has too much money in "her" bank account. She has been "edited out" of her entitlement to a decent subsistence. (8)

Cost Effective?

Against this toll of human agony, we must weigh the government's claims to vast savings because of computer matching. Based on my experience in government and on the lack of details provided by Inspectors General, I suspect that the figures are highly inflated. Government agencies generally include in the claimed savings the amount of benefits that would flow in the remaining lifetime of a beneficiary if the "hit" is confirmed, if the violator is located, if the violator has no defense, if the government can prove its case, and if the government can control its computers adequately to prevent future payments from being mailed. There are too many if's involved, and I have urged this subcommittee to conduct its own inquiry into the cost effectiveness of these programs. Until there is an unbaised appraisal, we are left with the figures announced by the government. After its massive 1977 iniative, HEW claimed a potential recovery of $100,000. This was less than the department spent on its 25th birthday celebration, according to journalist Evan Hendricks, who has effectively documented the abuses in matching. (9)

The effect (if not the intent) of computer matching is not to diminish waste and fraud but to push people off the welfare rolls. There is little evidence that the government is using the matching technique to go after more affluent beneficiaries, where the recovered amounts might be larger.

Some Matches Legitimate

None of the opponents of computer matching of whom I am aware are denying the legitimacy of the following programs: A government agency using personal information within its own organization to verify information on eligibility. A government agency matching files in another agency with the informed consent of the persons involved. A government agency checking lists of beneficiaries against lists of known dead persons. (A right to privacy action dies when the individual dies.) A government agency's proper use of the "law enforcement" exemption in the Privacy Act to exchange personal information once a suspicion of wrongdoing has arisen. The legislative history of the Privacy Act shows that this sort of exchange was clearly contemplated.

Participating in a government assistance program itself, whether it is Supplemental Security Assistance, a veterans loan, an agriculture support program, public assistance, education grants, or a grant for overseas travel, should not give rise to any suspicion. It is a status, not a crime. To subject a whole class of citizens to a search for possible violations is akin to a "general warrant," a practice in England that permitted the Crown to search without specifically naming its target. The framers of the Fourth Amendment to the U.S. Constitution were well aware of the practice (which was banished in England at about the same time) and sought to avoid such "fishing expeditions" by the American government. Even when the public need is compelling, government may not conduct a general search. If a crime is committed in a particular neighborhood, police may not search every dwelling there for clues. Police must secure a warrant "particularly describing the place to be searched, and the persons or things to be seized." (10) Inconvenient? Costly? Inefficient? Of course. Knowledgeable Americans know that the Bill of Rights is an obstacle to effective and aggressive law enforcement. It is a price we pay for freedom in our "person, houses, papers and effects." On the same theory, the government ought not be permitted to conduct a general search of all welfare recipients, or any other class of citizens, because it is aware of possible violations committed by unknown persons. Inconvenient? Costly? Inefficient? Of course.

Fighting Fraud Effectively

Does this leave government powerless to fight fraud and waste aggressively? Not at all. Studies by the government itself have shown that there are several more suitable procedures, if government agencies are truly serious about diminishing fraud. (In fact, government agencies seem more interested in intimidating people with a computerized/publicized blitz and in persuading Congress that they are actually doing something about fraud.)

The Attorney General's Federal Advisory Committee on False Identification in 1976 had this to say about welfare fraud: "Our surveys have shown that, due to the lack of identification standards for welfare recipients, neither Federal nor state agencies have a very good idea who is receiving almost $37 million per year in public assistance and Social Security payments." It said that a large part of the fraud problem was due to multiple collection of benefits by individuals using several identities. No computer matching (of data from separate agencies) is necessary to get at this part of the problem. Another significant factor in welfare fraud, the committee said, is check forgery — "about 16 percent of the total public welfare budget in Philadelphia for the year 1972." No computer matching is necessary to get at this part of the problem. The committee found that fraud in Social Security and Medicare programs — "remarkably low compared to the immense level of payments" — was due largely to the use of false identification at the application and collection stage. No computer matching is necessary to get at this part of the problem. The False ID Committee said, "We can only conclude that false identification fraud in welfare programs, like other types of program abuse, is most prevalent where there is the least effort to discover and punish it. We also find that such laxness is encouraged by the failure of Federal agencies to provide effective ID standards for welfare recipients, and failure to enumerate instances of suspected fraud uncovered in audits of state welfare programs and to take action against states which make no effort to deter such abuse." (11)

Apparently concerned about the problem, the National Institute of Justice in the Department of Justice ordered a report on "Fraud in Government Benefit Programs: Suggested State/Local Prevention Strategies." Throughout the 91 pages of suggested strategies in this 1982 report, there is not a word about computer matching. Instead, the private study says, "Preventive approaches to fraud problems are likely to have much higher returns than retroactive approaches. This is a point made throughout this report. By actively trying to identify fraud problems, agencies can not only uncover a higher proportion of existing fraud cases but also locate and correct problems in program design and implementation which facilitate frauds in the first place." (12)

Later it said, "It must be recognized that 'old fashioned' good management is the best single preventive measure," and included in that category, reorganization, training, proper staffing, sharing of administrative information, and corrective action.

In all the literature of the President's Council on Integrity and Efficiency, the total stress is on inflated claims of dollars recovered, not on changes made in agency procedures to prevent identical abuses in the future.

Preventive Measures

Advocates for privacy and for indigent persons are not asking that government officials let abuse continue. We all agree that abuse lessens public confidence in these programs and takes away resources from those who most need them. We are asking for government officials to confront the problem directly, with time-tested methods for determining eligibility. We are asking them to use common sense in evaluating applications. (To have a government social worker assume the role of helper and advise the applicant to bend the rules a bit and then to have a faceless bureaucrat declare later that his computer interprets the rules strictly seems unfair.) We are asking them to evaluate where abuse is most significant and to alter procedures so that it can be prevented in the future.

We are asking them to use the match programs that can work and that do not violate the Privacy Act or invade personal privacy. An example is the National Driver Register, which the current administration strangely sought to close down. The register compares personal information that was submitted for compatible purposes (to receive a driver's permit) and so it does not violate the letter or spirit of the Privacy Act. But the register has never been managed nor funded in a way so as to keep disqualified drivers off the highways.

We are asking government agencies to go after abuse in government programs that benefit the affluent, as well as the debt-ridden.

And we are asking them to comply with the Privacy Act.

As originally proposed in the Senate, the act would have provided for no exchanges of personal data among federal agencies without the consent of the individual. The report of the Senate Committee on Government Information in 1974 said of the act, "It is thus expected to exert some check on excessive or illegal reach of governmental power over the individual, and on illegal or inadvertent centralization of investigative programs and linkage of Federal data banks with those in the State and local governments and the private sector....It is designed to assure, in the future, that one government agency does not use the personal information given by the individual or by third parties to another agency to make what might be a detrimental decision affecting qualifications, rights, benefits, privileges or status without provision for notice of the existence of the information and obtaining consent, thereby allowing an opportunity to challenge its accuracy and reliability." (13)

The House of Representative Committee on Government Operations, however, agreed to permit certain exchanges for a routine use of the information, stating clearly, "A 'non-routine' transfer is generally one in which the personal information on an individual is used for a purpose other than originally intended."

The committee report on the bill said also, "The Committee intends to exercise a vigorous oversight check on agencies to make certain as much as possible that no 'non-routine' transfers of records of the type requiring prior written consent are either hidden or blanketed in under the 'routine' category to nullify the basic protections of the law to individuals." (14)

Throughout the Senate and House debates, it is repeated that the "routine use" exception was intended to permit federal agencies to make certain data exchanges necessary for "housekeeping." The Office of Management and Budget repeated this definition in promulgating guidelines for federal agencies to comply with the Privacy Act. (15)

When the Department of Health, Education and Welfare in 1977 sought payrolls of federal employees from the Civil Service Commission and the Department of Defense, both agencies were reluctant to make the disclosures because of the strictures of the Privacy Act. The Commission general counsel told HEW in a letter, "It is evident that this [payroll] information on employees was not collected with a view toward detecting welfare abuses. Secondly, and perhaps more significantly, at the matching state there is no indication whatsoever that a violation or potential violation of law has occurred. It is only after a comparison of data between those currently on Federal payrolls and AFDC rolls produces a 'match' that a possible or potential violation of law warranting further inquiry is evident. It cannot fairly be said, therefore, that disclosure of information about a particular individual at this preliminary state is justified by any degree of probability that a violation or potential violation of law has occurred." (16) Then, in legal reasoning that is as convoluted as any the executive branch has seen, the General Counsel of the Civil Service Commission in his memorandum said that the Freedom of Information Act, and therefore the Privacy Act under subsection (b)(2), would require disclosure of the payroll information. Was the general counsel seriously arguing that his date of birth, Social Security number, salary and duty location — and those of thousands of other federal employees — are available to me under the Freedom of Information Act?

The Department of Defense didn't want to disclose employee information either because of its responsibilities under the Privacy Act, but lest it appear to be sheltering welfare cheaters, it agreed that the "routine use" exception would permit the disclosure for Project Match. (17)

Only after the matches had been done and after hundreds of public assistance recipients and federal employees had been subjected to anxiety and embarrassment did the Office of Management and Budget issue guidelines that sought to legitimize matching under the Privacy Act. One would think that the Privacy Act and fundamental fairness would at least permit these victims of computer matching to examine the data and challenge its accuracy if appropriate. That is the requirement of subsection (d)(1). But the Inspector General of Health and Human Services, in proposals published this year, now intends to exempt information in his office from this basic requirement. (18) That means that any "hits" that remain in the files of the Inspector General may not be inspected by a citizen who has reason to believe he or she has been victimized by mistaken identity, error or misinterpretation. This brings us back to the situation we experienced prior to passage of the Privacy Act, when federal agencies freely exchanged personal data without the knowledge of the individual and without opportunity for the individual to challenge its accuracy.

I urge this subcommittee to probe completely into the conduct of computer matching, to inform the public of the true cost effectiveness of the programs and of the cost to individual liberties, and to make clear to the Executive Branch that certain matches are simply not permissible, because of the Privacy Act, the Constitutional right to privacy, and the Fourth Amendment to the Constitution.

In 1928, Justice Louis D. Brandeis was confronted with a governmental invasion of privacy made possible by new technology. In a notable dissent to the Supreme Court's approval of wiretapping, Justice Brandeis wrote that the makers of our Constitution "conferred, as against the government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." (19) In a phrase that was later invoked in the legislative debate on the Privacy Act and that could apply to today's enthusiasts of computer matching, Brandeis said also,

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachments by men of zeal, well-meaning but without understanding.

FOOTNOTES

1. "The Dimensions of Privacy" by Louis Harris & Associates (Stevens Point, Wisc.: Sentry Insurance, 1979), p. 80.

2. Remarks by Richard P. Kusserow at Symposium on Privacy/Freedom of Information Policy, American Association of Access Professionals, Nov. 18, 1982.

3. "How Not to Catch Welfare Cheaters" by Evan Hendricks, The Washington Post, July 1, 1979, p. C 8.

4. Privacy Journal, Washington, D.C., Oct. 1982, p. 4.

5. Committee on Government Operations, U.S. Senate and House of Representatives, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974 at 859-60 (Joint Comm. Print 1976).

6. From an interview with Alan Rodgers of the Massachusetts Law Reform Institute in Boston, which represents welfare recipients in the cases of 15,844 Welfare Recipients v. King, CA79-643-G (D., Mass. 1979) and Lessard v. Spirito, CA82-3389-MA (D. Mass. 1982).

7. Ibid.

8. Ibid. This represents a composite of typical cases.

9. "How Not to Catch Welfare Cheaters."

10. Fourth Amendment to the Constitution.

11. U.S. Department of Justice The Criminal Use of False Identification, Report of the Federal Advisory Committee on False Identification at 47, 1976.

12. U.S. Department of Justice National Institute of Justice Fraud in Government

Benefits Programs: Suggested State/Local Prevention Strategies at 5, 1982.

13. Legislative History of the Privacy Act of 1974 at 221.

14. Ibid. at 305.

15. Ibid. at 1030.

16. Letter from Carl F. Goodman, General Counsel, U.S. Civil Service Commission, to Charles Ruff, Acting Deputy Inspector General, Department of Health, Education, and Welfare, July 27, 1977.

17. Memorandum of Understanding between Robert P. Bedell, Assistant General Counsel, Office of Management and Budget, and William P. Cavaney, Executive Secretary, Defense Privacy Board, in the files of the Committee on Government Operations Subcommittee on Government Information and Individual Rights, House of Representatives.

18. See 47 Fed. Reg. 43099 (Sept. 30, 1982).

19. Olmstead v. U.S., 277 U.S. 438 (1928) (dissenting opinion).

TESTIMONY OF RONALD L. PLESSER, FORMER GENERAL COUNSEL OF THE U.S. PRIVACY PROTECTION STUDY COMMISSION, BEFORE THE U.S. SENATE SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT

December 15, 1982

Senator Cohen and members of the Subcommittee, my name is Ronald L. Plesser. I am a practicing lawyer in the District of Columbia and I had the privilege of serving as General Counsel to the U.S. Privacy Protection Study Commission. Since 1977 when the Commission completed its work, I have served as a reporter to the National Commission in Uniform State Law's Fair Information Practices committee and I have litigated several Privacy Act cases. I have been asked to testify here today to give my view of the Privacy Act of 1974 and, in particular, the enforceability of that statute in the context of matching programs.

My view of matching is somewhat colored by my recent experience working with the Privacy Act. I believe that the Privacy

Act, with the exception of its access to records and correction of records provision, is essentially unenforceable. Therefore, reliance upon that Act to protect privacy interests are by and large misplaced. I will detail the basis for this conclusion, but first I would like to present a context for this discussion.

No one can attack the motives of matching programs. The elimination of fraud and abuse from public financial assistance programs is a goal not to be questioned. What can be questioned, however, is the means of reaching the goal. In examining matching programs, a review of the state of Fourth Amendment rights will help view the principles of privacy. This examination inevitably leads to the conclusion that the Constitution gives little, if any, protection to an individual and that we must look to legislative solutions, governmental mechanisms and Congressional oversight to protect the interests of privacy in our society.

The Privacy Commission's ability to conceptualize the problem it was trying to face in looking at an individual's right to control information maintained about individuals was facilitated by a case entitled Miller v. U.S., 425 U.S 435 (1976) issued by the Supreme Court in the midst of the Privacy Commission's deliberations. The Miller story still had two lessons which are still of importance. First, the Fourth Amendment probably cannot survive the technological age and, second, that only by the protection of the rights of those in contct with the law can we protect the rights of all. Mitchell Miller's story bears repeating. An agent from the U.S. Treasury Department's Bureau of Alcohol, Tobacco and Firearms suspected Miller of direct involvement in two events, a seized truck and a warehouse fire which indicated illegal manufacture of alcoholic products. Two weeks later, the agent presented grand jury subpoenas to the two banks where Miller maintained accounts. Without notifying Miller, copies of his checks and bank statements were either shown or given to the Treasury agents as soon as they presented the subpoenas. The subpoenas did not require immediate disclosure, but the bank officers nonetheless responded at once.

After he had been indicted, Miller attempted to persuade the court that the grand jury subpoenas used by the Treasury Department were invalid and, thus, the evidence obtained with them could not be used against him. He pointed out that the subpoenas had not been issued by the grand jury itself, and further, that they were returnable on a day when the grand jury was not in session. Finally, Miller argued that the Bank Secrecy Act's requirement that banks maintain microfilm copies of checks for two years was an unconstitutional invasion of his Fourth Amendment rights. The trial court rejected Miller's arguments and he appealed.

The Fifth Circuit Court of Appeals also rejected Miller's claim that the Bank Secrecy Act was unconstitutional, an issue that had already been resolved by the U.S. Supreme Court in 1974. The Court of Appeals agreed, however, that Miller's rights, as well as the bank's, were threatened and that he should be afforded the right to legal process to challenge the validity of the grand jury subpoenas. The Court of Appeals saw Miller's interest in the bank's records as deriving from the Fourth Amendment protection against unreasonable searches and seizures which protected him against "compulsory production of a man's private papers to establish a criminal charge against him."

On April 21, 1976, a fateful day for personal privacy, the U.S. Supreme Court decided that Mitchell Miller had no legitimate "expectation of privacy" in his bank records and thus no protectible interest for the Court to consider. The Court reasoned that because checks are an independent record of an individual's participation in the flow of commerce, they cannot be considered confidential communications. The account record, moreover, is the property of the bank, not of the individual account holder. Thus, according to the Court, Miller's expectation of privacy was neither legitimate, warranted, nor enforceable.

Since the Privacy Commission's report, the Congress enacted the Right to Financial Privacy Act, which to a limited extent, gives depositors some standing to challenge Federally-issued subpoenas. The Supreme Court's conclusion that Miller could do nothing to protect records about him has not changed. But for the promise of legislative solutions individuals have less and less control over information maintained about them. The Constitutional protections of the Fourth Amendment continue to be eroded and soon little will be left.

In matching programs there are no Fourth Amendment protections. Searches of the records of individuals are no longer limited by the word reasonable as envisioned by the framers of the Constitution. The technology of computers have sanitized search and seizures. Match programs search information about individuals to the same end as if a government agent broke into your house and rifled through your papers. But because you can't see it and because the ends are justifiable, the Fourth Amendment is deemed irrelevant. Not only in matching, but in other forms of computer activity, the Fourth Amendment is fast becoming a dead principle.

That brings us back to the Privacy Act as legislative protection in lieu of Fourth Amendment protection. The supporters of match programs rely upon the Privacy Act as the counterbalancing means for the protection of personal privacy. The revised OMB guidelines state "If the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, it may proceed to make the disclosure to the matching agency." That and the testimony we have heard today implies that the Privacy Act is a reliable and effective replacement for traditional Fourth Amendment protections.

I am afraid that, in the matching context, the Privacy Act fails for two reasons. First, the routine use provision, which requires that a Federal agency use information only in a manner which is compatible with the purposes for which the information was originally collected is subject to broad interpretation. Unless strictly enforced, agencies have demonstrated a tendency to interpret this to mean a wide category of uses, including disclosure to private individuals, non-federal agencies and to the press. These interpretations allow broad discretion by agencies to determine when and to whom disclosures of selected information are made. My fellow panelists this morning contend that many matches violate the routine use of provisions of the Privacy Act. I agree with them. The problem, however, is are there any means to limit the breadth of interpretation and broad discretion illustrated by the routine uses adopted by many agencies. The answer is that under current law there is little that can be done.

The Privacy Act, to large extent, is unenforceable. Most courts faced with the issue have stated that the Privacy Act contains no injunctive relief. Cell Associates, Inc. v. N.I.H., 579 F.2d 1155 (9th Cir. 1977); Parks v. U.S. Internal Revenue

Service, 618 F.2d 677 (10th Cir. 1980). That means that a court under the Privacy Act cannot stop an agency from violating the Privacy Act. A court can enforce an individual's right to see and correct records, but that is all it can require. There is a damage-recovery provision where an individual may recover damages against the government for violations of the Act. However, in order to obtain a judgment the plaintiff must demonstrate that the government acted in an intentional or willful manner, that the violations adversely affected the individual and that the individual suffered out-of-pocket loss. Recovery is limited to out-of-pocket loss and no recovery for emotional loss or mental injury is compensable. In one recent case. a Court has gone even further by directing that recovery can be had only upon the showing of substantial physical injury. Albright v. U.S. (copy of District Court Order attached). To demonstrate physical injury, a plaintiff must have the imagination of a George Orwell.

In a matching program even if an agency has clearly violated the Act, the effectiveness of a remedy is severely limited.

The tragedy, however, is that there is no one in the government with the role of enforcing or even overseeing privacy standards. The privacy officers in agencies stand as lonely voices. Only the Department of Defense has institutionalized privacy protection with its Defense Privacy Board staffed by high-level civilians and military officers. The OMB has some responsibilities, however, their prime mission is the elimination of fraud and abuse and not privacy protection.

The Privacy Commission recommended a permanent Privacy Commission, whose role would be to monitor and advise as to the implementation of privacy rights in the Federal sector. That recommendation was never seriously considered by Congress and the Administration, because of the fear of more bureaucracy. The National Telecommunications and Information Administration (NTIA) fulfilled that role for several years. Their role, however, has been drastically reduced and they no longer can be relied upon to represent a privacy constituency. Perhaps the debate on match and the coming of 1984 can serve an important function by reawakening us all to the interests of privacy and the need of constant vigilence. That vigilence should be institutionalized so that that these issues can be rationally resolved before all privacy protections are lost. Moreover, the Privacy Act itself should be re-examined. It is costly to administer and it delivers little in terms of real protection. A re-evaluation of that Act may go a long way towards resolving the concerns raised by matching programs.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL T. ALBRIGHT, et al.,	:	
Plaintiffs,	:	
v.	:	Civil Action No. 78-0397
UNITED STATES OF AMERICA, et al.,	:	FILED
Defendants.	:	DEC 1 1982

CLERK, U.S. DISTRICT COURT
DISTRICT OF COLUMBIA

FINDINGS OF FACT AND CONCLUSIONS OF LAW OF UNITED STATES DISTRICT JUDGE CHARLES R. RICHEY

Plaintiffs brought this action under the Privacy Act of 1974, 5 U.S.C. §552a. They alleged that defendants violated subsection (e)(7) of the Privacy Act, 5 U.S.C. §552a(e)(7) (1976), by videotaping a meeting held for analysts with the Bureau of Hearings and Appeals of the Social Security Administration, United States Department of Health and Human Services,[1] and attended by analysts, supervisors and union officials. On February 14, 1979, this Court granted defendants' motion for summary judgment holding, inter alia, that there was no violation of the Privacy Act since the videotape was not placed in a system of records within the agency.

On July 17, 1980, the Court of Appeals reversed this Court's decision, holding that Section (e)(7) of the Privacy Act does apply because the videotape was a record of the exercise of First Amendment rights and therefore its creation came within the terms of the Privacy Act. Albright v. United States, 631 F.2d 915 (D.C. Cir. 1980). The Court remanded for a determination as to whether plaintiffs could prevail on their claim under the Act, and set forth three findings that had to be made in plaintiffs' favor in order for them to pevail: (1) whether plaintiffs were depicted by voice or picture on the videotape; (2) whether plaintiffs could establish that the Court had jurisdiction by demonstrating that the "making of this record had an adverse effect on them as required by Subsection (g)(1)(D) of the Act;" and (3) whether plaintiffs could establish entitlement to a damages remedy by establishing that "the agency acted in a manner which was intentional or willful." 5 U.S.C. §552a(g)(4). 631 F.2d at 921. The Court of Appeals stated that, as to the damages remedy, the defendants had stated three contentions which, if found to be true, raised "serious doubts as to whether the agency action was a willful and intentional violation of the Act which would justify the assessment of damages." Id. These were that: (1) the agency made the videotape in order to preserve a record for other affected analysts who would not be able to attend the meeting; (2) the idea to record the meeting originated from an analyst; (3) the agency volunteered to destroy the videotape when it became aware that analysts objected to it, but that plaintiffs' union refused the offer. Id.

---

[1] HHS was formerly designated the Department of Health, Education and Welfare, 20 U.S.C.A. §3508 (Supp. 1982).

On October 28, 29 and November 1, 1982, an evidentiary hearing was held before the Court on these issues. At the conclusion of plaintiffs' case, the government moved for an involuntary dismissal pursuant to Rule 41(b) of the Federal Rules of Civil Procedure on the ground that upon the facts and the law plaintiffs had demonstrated no right to relief. After hearing full argument of counsel for the parties and reviewing the entire testimony and evidence presented by plaintiffs, this Court granted the government's motion to dismiss. The Court now enters the following findings of fact and conclusions of law pursuant to Rule 52(a) of the Federal Rules of Civil Procedure.

FINDINGS OF FACT

1. Plaintiffs, Michael T. Albright, Tiiu A. Anniko, Rae Balest Chamberlain, Earnest Baskerville, Michael E. Bryant, George C. Condern, Devarieste Curry, Melvin F. Daniels, John D. DiLillo, Donald Gregory, Judy A. Gregory, Dolly A. Marshall, John A. Martone, Yvonne P. Porter, Tommie L. Smith, Glenda Walker, and Anna Wong, are present or former Hearings and Appeals Analysts at the Arlington, Virginia Office of the Bureau of Hearings and Appeals (BHA), Social Security Administration (SSA), United States Department of Health and Human Services (HHS).

2. The defendants are the United States of America and the following persons, who are sued in their official capacities:

(a) Richard D. Schweiker, successor to Joseph Califano, an original defendant as Secretary of HHS;
(b) John A. Svahn, as Commissioner of the Social Security Administration;
(c) Louis Hayes, as the Director of BHA;
(d) Orlando MacGruder, as the Assistant Bureau

Director (Office of Management Systems),
Division of Administration, BHA;
(e) Hinda Silver, as the Personnel Officer of
BHA. [2/]

3. In the summer of 1977, BHA made a preliminary determination to reclassify GS-13 BHA analyst positions to a GS-12 level.

4. In July, 1977, BHA temporarily withheld promotions of BHA analysts from GS-12 to GS-13 levels. By September, 1977, twenty-four promotions had been recommended and withheld.

5. On September 9, 1977, Mr. Makoff who was then the Personnel Director of BHA, met with the union representatives of the BHA analysts to inform them that Mr. Robert L. Trachtenberg, Director of BHA, had affirmed the determination to reclassify the BHA GS-13 analyst positions to GS-12 and had imposed a moratorium on all such promotions to GS-13.

6. At the request of union representatives, Mr. Makoff scheduled and held a meeting on September 23, 1977 with BHA analysts to discuss the reasons for the reclassification decision and the moratorium on promotions to GS-13 which had been imposed.

7. Prior to the September 23rd meeting, several affected analysts contacted Mr. Robert Silliman, a BHA Labor Relations official to request that the meeting be rescheduled because they could not attend the meeting. One such analyst, Ms. Vivienne Evans, requested that a representative

---

2 When suit was filed, it named the individuals who then occupied these posts. Pursuant to Rule 25(d) of the Fed.R.Civ.P., when a public official is sued in his official capacity, his successor in office is automatically substituted as a party.

attend in her place, and that the representative be permitted to "tape cassette" the meeting. Mr. Silliman informed Mr. Makoff's office of Ms. Evans' call and other similar requests he received.

8. Mr. Makoff arranged for the meeting to be videotaped. Testimony of plaintiffs and Robert Silliman.

9. Approximately forty BHA analysts, four of the five immediate BHA supervisors, other management personnel, the union president and other union representatives attended the September 23rd meeting. No restriction was placed on who could attend the meeting.

10. The videotape camera was sitting on a large tripod located near the back of the room and was or should have been conspicuous to all who entered.

11. Several analysts and others situated in the back of the room including several of the plaintiffs observed the camera and the television monitor at the commencement of the meeting.

12. The meeting, which was videotaped, lasted approximately forty-five minutes.

13. Three plaintiffs, Melvin Daniels, Donald Gregory and John Martone, are not depicted either by voice or by picture on the videotape. All other plaintiffs depicted visually and/or orally on the videotape.

14. Three plaintiffs, Rae Balest Chamberlain, George Condern and Dolly A. Marshall, sustained no adverse effect as a result of the videotaping. To the extent that any of these three plaintiffs

testified as to any effect, the allegations were of some form of emotional distress wthout any out-of-pocket loss or physical injury. No credible evidence was adduced demonstrating that any of these effects were the result of the videotape.

15. Plaintiffs Tiiu A. Anniko, Earnest Baskerville, Michael E. Bryant, Devarieste Curry, John D. DiLillo, Judy A. Gregory, Yvonne P. Porter, Tommie L. Smith, and Glenda Walker each stated that the only adverse effect that they suffered as a result of the videotaping consisted of some form of emotional trauma, anger, fright or fear that they might be identified as malcontents within BHA. None of these plaintiffs provided credible evidence that the adverse effects they alleged were the result of the videoptaping.

16. No physician testified as to any effect or injury alleged by any plaintiff. Nor did any of the plaintiffs introduce any medical testimony which demonstrated that any alleged injury or harm was the result of the videotaping. Testimony of plaintiffs.

17. Two plaintiffs, Michael Albright and Anna Wong, claimed out-of-pocket expenses for exacerbation of pre-existing medical conditions. Michael Albright claimed that his pre-existing neurological problems were exacerbated and Anna Wong claimed that her allergy condition was exacerbated. Neither provided any credible evidence that the videotaping caused the exacerbation of an existing illness. No physician testified on behalf of either

plaintiff that there was an exacerbation of their pre-existing condition as a result of the videoptaping. Neither plaintiff offered credible evidence of any out-of-pocket expenses as a result of the videotaping nor did they offer other evidence to sustain their burden of proof in this regard.

18. No plaintiff suffered any physical injury as a result of the videotaping.

19. No plaintiff introduced any credibile evidence establishing actual damages or out-of-pocket losses directly attributable to the videotaping and all admitted as much.

20. The Court finds that the agency did not act in a manner which was "intentional" or "willful." The agency made the videotape so that oher analysts who were unable to attend could see what happened at the meeting. The idea to record the meeting actually came from an analyst.

21. BHA offered to destroy the videotape when it became aware that some of the analysts were "upset" that it had been made.

22. The analysts' union, which was their duly authorized representative, refused the offer because it wanted to preserve a record of the videotape. The union sought to preserve the videotape because of the dispute between the parties and as evidence for any future legal action.

23. Moreover, the plaintiffs who saw the videotape equipment could have left the room at any time had they desired.

CONCLUSIONS OF LAW

1. The jurisdiction of the Court is conferred under the Privacy Act of 1974, Title 5, United States Code §552a(g)(1)(D) and Title 28, United States Code §1331(a).

2. In considering a Rule 41(b) motion pursuant to the Federal Rules of Civil Procedure at the close of plaintiffs' case-in-chief, the Court, in a non-jury case, is not required to draw inferences in the plaintiffs favor at this stage of a case such as this or even concern itself with whether the plaintiffs have made out a prima facie case notwithstanding some dicta in some related fields, Wright & Miller, Federal Practice and Procedure. Civil § 2371, at 224-225. See also Woods v. North American Rockwell Corporation, 480 F.2d 644, 645-646 (10th Cir. 1978); Ellis v. Carter, 328 F.2d 573, 577 (9th Cir. 1964). Rather, the court is required to weigh all the evidence, resolve any conflicts and, to decide itself where the preponderance lies. Id. Accordingly, the Court hereby grants the defendants' Rule 41(b) Motion.

3. The only remedy in an action such as this under subsection (g)(1)(D) of the Act, 5 U.S.C. §552a(g)(1)(D), is the damages provision set forth in subsection (g)(4)(A), 5 U.S.C. §552a(g)(4)(A), which permits recovery only for "actual damages sustained by the individual . . . but in no case shall a person entitled to receive less than the sum of $1,000." 5 U.S.C. §552a(g)(4)(A).

4. Actual damages under the Privacy Act are limited to "out-of-pocket" expenses and do not include damages for emotional trauma, anger, fright or fear. Houston v. United States Department of Treasury, 494 F. Supp. 24, 29-30 (D.D.C. 1979). See also Garber v. United States, 578 F.2d 414, 415 (D.C. Cir. 1978); Morgan v. District of Columbia, No. 79-588 n.20 (D.C. App August 31, 1982); District of Columbia, 436 A.2d 1294, 1296 (D.C. App. 1981).

5. Accordingly, no plaintiff can recover any damages for emotional trauma, anger, fright, fear or similar emotions without a showing of out-of-pocket loss.

6. Plaintiffs, Melvin Daniels, Donald Gregory, and John Martone are not depicted on the videotape. Accordingly, they have failed to establish that any record of their exercise of a First Amendment right, as covered by subsection (e)(7) of the Privacy Act, 5 U.S.C. §552a(e)(7) (1976), was maintained and their claims are dismissed, with prejudice.

7. Plaintiffs, Rae Balest Chamberlain, George Condern and Dolly A. Marshall are depicted visually and/or orally but have not demonstrated any adverse effect as required by subsection (g)(1)(D) of the Privacy Act, 5 U.S.C. §552(g)(1)(D). Accordingly, their claims are dismissed, with prejudice.

8. Plaintiffs, Tiiu Anniko, Earnest Baskerville, Devarieste Curry, John DiLillo, Judy Gregory, Yvonne Porter, Tommie Smith, and Glenda Walker are depicted orally or visually on the videotape, but they have failed to establish any adverse effect as required by subsection (g)(1)(D) of the Privacy Act, 5 U.S.C. §552a(g)(1)(D) (1976). The Court finds that these plaintiffs have no out-of-pocket expenses and suffered no physical injury and thus are dismissed, with prejudice.

9. As for any damages for out-of-pocket expenses for exacerbation of pre-existing medical conditions claimed by Michael Albright and Anna Wong, the Court concludes that the evidence fails to show any out-of-pocket expenses or physical injury directly attributable to the videotaping. Neither plaintiff suffered any exacerbation of any pre-existing condition, suffered any physical injury or suffered any out-of-pocket loss attributable to the videotaping. Consequently, neither plaintiff has established a right to recover any damages pursuant to subsections (g)(1)(D) and (g)(4)(D)(g)(4)(A) of the Privacy Act. 5 U.S.C. §§552a(g)(1)(D) and (g)(4)(A).

10. The Court finds that to the extent that plaintiffs Michael Albright and Anna Wong have suffered anger and emotional distress which they contend is attributable to the videotaping, both plaintiffs have failed to establish an adverse effect as required by subsection (g)(1)(D) of the Act to vest jurisdiction in this Court. Accordingly, their claims are dismissed, with prejudice. See Albright, 631 F.2d at 921.

11. Assuming, arguendo, that any plaintiffs suffered emotional distress which may be attributable to the videotaping, the Court finds that no plaintiff incurred a physical injury. Accordingly, regardless of whether plaintiffs incurred out-of-pocket losses, under the law of the District of Columbia, damages for emotional distress resulting from negligence is precluded in the absence of substantial physical injury . Garber v. United States, 578 F.2d 414, 415 (D.C. Cir. 1978); District of Columbia v. Smith, 436 A.2d 1294, 1296 (D.C. App. 1981).

12. Further, the Court has found that the idea to record the meeting actually came from an affected analyst who could not attend. BHA decided to make this videotaped recording for analysts who could not attend the meeting, and BHA offered to destroy the videotape when it became aware that the analysts were "upset" that it had been made but the analysts' union refused the offer. Thus, the Court concludes that plaintiffs have failed to establish that the agency acted in a manner which was intentional or willful as required by 5 U.S.C. §552a(g)(4). Albright, 621 F.2d at 921 (D.C. Cir. 1980); Bruce v. United States, 621 F.2d 914, 917 (8th Cir. 1980).

13. Accordingly, the Court concludes that there has been no violation of the Privacy Act, 5 U.S.C. §552a.

14. In accordance with the offer previously made by defendants this Court directs that the videotape at issue

and any copies thereof be destroyed following exhaustion of all appellate remedies in this case.

15. Any finding of fact deemed to be conclusion of law is adopted as such. Conversely, any conclusion of law deemed to be a finding of fact is also adopted as such.

CONCLUSION

Pursuant to Rule 58 of the Federal Rules of Civil Procedure, judgment by separate order of this date is to be entered for the defendants and the action is to be dismissed, with prejudice. Costs shall be awarded in favor of the defendants and against the plaintiffs who brought this case.

Entered: November 30, 1982

Charles R. Richey
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL T. ALBRIGHT, et al., :
Plaintiffs, :
v. : Civil Action No. 78-0397
UNITED STATES OF AMERICA, et al., :
Defendants :

ORDER

This case came before the court for an evidentiary hearing on October 28, 29, and November 1, 1982 following remand from the Court of Appeals for this Circuit. At the conclusion of plaintiffs' presentation of their evidence on November 1, 1982, this court granted defendants' motion for involuntary dismissal pursuant to Rule 41(b) of the Federal Rules of Civil Procedure and dismissed plaintiffs' claims brought under Subsection (e)(7) of the Privacy Act. 5 U.S.C. §552a(e)(7). In accordance with that ruling, it is, by this Court, this 30 day of November, 1982,

ORDERED, ADJUDGED AND DECREED in accordance with the Court's findings of fact and conclusions of law filed of even date herewith that judgment be entered for the defendants and that this action be dismissed with prejudice with costs awarded against the plaintiffs, and it is further

ORDERED, ADJUDGED AND DECREED that the videotape at issue in this case, marked as Joint Trial Exhibit One shall be maintained in the possession of the Office of the Clerk of this Court until the plaintiffs' rights of appeal have been fully exhausted, at which time the tape and any copies thereof shall be destroyed, and it is further

ORDERED, ADJUDGED, AND DECREED that plaintiffs' Motion for Stay Pending Appeal is denied as moot.

Date: November 30, 1982.

Charles R Richey
Charles R. Richey
United States District Judge

Senator COHEN. The subcommittee will stand adjourned until tomorrow at 9:30.

[Whereupon, at 12:45 p.m., the hearing was adjourned, to reconvene at 9:30 a.m., Thursday, Dec. 16, 1982.]

OVERSIGHT OF COMPUTER MATCHING TO DETECT FRAUD AND MISMANAGEMENT IN GOVERNMENT PROGRAMS

THURSDAY, DECEMBER 16, 1982

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT
OF GOVERNMENT MANAGEMENT,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, D.C.

The subcommittee met, at 9:35 a.m., in room 3302, Dirksen Senate Office Building, Hon. William S. Cohen (chairman of the subcommittee) presiding.

Present: Senator Cohen.

OPENING STATEMENT OF SENATOR COHEN

Senator COHEN. The hearing will come to order.

Today, the Oversight of Government Management Subcommittee will continue its hearings on the implications of the widespread use of computer matching to detect waste, fraud, and mismanagement in Government programs.

Our hearings are exploring the issue of how we can strike the proper balance between the goals of Government efficiency and personal freedom.

We learned at our hearing yesterday that computer matching has mushroomed in recent years, and like mushrooms, which grow best in the dark, computer matching has flourished with little light or examination of its consequences. Insufficient oversight and inadequate thought have been given to the need for standards to insure that computer matching does not compromise the privacy rights of individuals. When used prudently, computer matching can be a valuable tool for revealing—and deterring—waste and fraud, but troubling questions about its use remain unanswered.

Our witnesses this morning include the General Accounting Office, representatives of State government, and a privacy expert. I am confident that their statements will add considerably to the subcommittee's examination of this complex issue.

Our first witness this morning is Wilbur D. Campbell, the Director of the Accounting and Financial Management Division of the General Accounting Office. The GAO has had many years of experience with matching in conjunction with various audits that it has conducted.

Mr. Campbell, would you please try and summarize your statement as best as possible, and then perhaps we can move on to some questions.

TESTIMONY OF WILBUR D. CAMPBELL, DIRECTOR, ACCOUNTING AND FINANCIAL MANAGEMENT DIVISION, GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY EDWARD M. GLAGOLA, COMPUTER SPECIALIST, ACCOUNTING AND FINANCIAL MANAGEMENT DIVISION; JAMES R. WATTS, GROUP DIRECTOR, AUTOMATIC DATA PROCESSING, ACCOUNTING AND FINANCIAL MANAGEMENT DIVISION; AND JOHN W. LAINHART, GROUP DIRECTOR, AUDIT OPERATIONS, HUMAN RESOURCES DIVISION

Mr. CAMPBELL. Thank you very much, Mr. Chairman.

We are here at your request to discuss the use of computer matching as a means for detecting and preventing error, waste, and abuse.

Based upon our experiences, as well as those of other Government agencies, we believe that computer matching can be a very cost-effective tool for detecting error and fraud in Government entitlement programs and for identifying actions needed to strengthen program controls. Even more important, as a form of internal control, it can be a very effective deterrent to fraud and waste if it is common knowledge that it is being used.

Funding for entitlement programs is projected at over $350 billion for 1983 and potential erroneous payments could run into the billions. Because computer matching is a relatively low-cost method of identifying and reducing erroneous payments, we endorse its use with the understanding that the rights of individual citizens will be protected as required by the Privacy Act of 1974 and the Tax Reform Act of 1976, and due-process provisions for reducing or eliminating benefit payments are followed.

For the most part, our efforts have focused on identifying erroneous payments rather than evaluating the cost-effective use of computer matching by Federal and State agencies. Our experiences with computer matching have shown that the benefits—namely, identifying and stopping erroneous payments and correcting program deficiencies—generally far outweigh the cost of a match.

As far back as 1976, for example, we made a computer match of supplemental security income payments with records of benefit payments made by the VA and the Railroad Retirement Board. By using a computer matching technique, we were able to identify and report total erroneous payments of more than $60 million annually. The Social Security Administration has now been conducting similar matches routinely, and we understand that in fiscal 1982 the savings actually exceed $100 million.

We reported in January 1982 that overpayments in five major needs-based benefit programs would probably exceed $1 billion in fiscal 1982. Since eligibility and the amount of these payments are dependent upon recipients' income and assets, increased verification of these data via computer matching could reduce significantly the number of erroneous payments.

The potential payback of a computer match can be significant, but the question remains: How much does it cost? The straightforward answer is that "it all depends," because there are so many variables. The costs will depend on such variable factors as the size and complexity of the records being matched, the quality and compatibility of the data in computerized files, and the extent of verification required following a match.

One element of cost is the cost of the software needed to make the match. This cost, by itself, can be large; however, once developed, the software can be used on many different matches. For example, our staff designed a set of computer programs for matching which we call Seeker; our development costs were about $100,000. To date, we have used it on several different audits in the GAO. Also, two executive agencies are using it now—the Veterans' Administration and the Department of Labor, and others are planning to use the program. On one matching project alone, we identified about $2 million in overpayments, of which about $500,000 has been collected.

Another element of cost is the cost of computer time to match the files. But here again, the cost is relatively insignificant in relation to the potential benefits. On a current audit, we spent less than $10,000 in computer time to match over 4 million records. The potential erroneous payments on the hits identified in this match may be several million dollars.

Some major operational problems can further increase the costs and time involved in computer matching. They involve incompatibilities in ways in which data is represented in computer files of different agency systems and inaccurate and unreliable data contained in their automated files. We have addressed both of these problems in several reports and although some progress has been made, much more needs to be done.

Because of the many variables involved, prudent program management requires that proposed matches be planned and properly justified and evaluated periodically in terms of costs and actual benefits. In assessing benefits, however, program managers both at the State and Federal level should view computer matching as a tool for preventing as well as detecting error and fraud and therefore, its use can act as a deterrent to program abuse.

In this context, computer matching can be viewed as an internal control technique, as well as a tool for evaluating the effectiveness of other internal controls. For instance, computer matching can be used before benefits are authorized to validate or verify eligibility related information provided by an applicant.

With regard to your question of when and how often computer matching should take place, the issue centers around whether it should be done in the prepayment stage or the postpayment stage, and if in the latter, how frequently?

Selective verification of critical eligibility factors through computer matching at the prepayment stage would have the obvious benefits of identifying potential program abusers and errors before erroneous payments are made, reduce expensive followup and collection activities and, as I stated earlier, act as a deterrent in preventing or reducing the amount of program abuse that may take place.

Because of changes in circumstances involving individual income, assets, dependencies, and the like, computer matches should also be considered for persons already receiving Federal benefits. Whether matches should be performed, and whether the match should be on a one-time or routine basis are dependent on several factors and should be considered on a case-by-case basis.

While there are advantages to using computers to verify data about persons applying for or already receiving Federal benefits, the Tax Reform Act of 1976, which was designed to protect the privacy rights of taxpayers, restricts or prohibits the matching of certain computerized data.

In January 1982, we recommended some legislative changes to facilitate computer matching in needs-based benefit programs. In these programs an individual's eligibility is based upon his or her income and assets. Our recommendations addressed the use for verification purposes of: One, wage and earnings data maintained by the States and SSA; and, two, unearned income data maintained by the Internal Revenue Service. However, the opening of Federal tax data for use in other Government programs involves certain policy considerations concerning privacy.

Wage data maintained by the States is generally considered to be the best available wage information for verification purposes. The States collect this information from employers to determine eligibility and benefits under the unemployment insurance program. However, there are a couple of limitations.

First, only 38 States have laws that require collection of quarterly wage data for use in the unemployment insurance program. The other 12 do not. Most get only gross payroll data from employers. The Department of Labor has recently drafted proposed legislation to respond to our recommendation to require all States to collect wage data quarterly.

Second, the data for all States does not include wages of Federal employees, military personnel, and earnings of the self-employed. SSA wage information is more comprehensive than State data because it does include these wages and earnings. A major problem, however, is that because these data are collected for Federal income tax purposes, as well as for the SSA's use, access to the data is controlled, for privacy reasons, by the Tax Reform Act of 1976. This law was enacted to provide stringent disclosure limitations on tax return data because of concerns about individual privacy. Although the Congress has passed separate legislation making the SSA's wage data available for use in the AFDC and food stamp programs, such data cannot be used for verification purposes in other Federal needs-based programs.

We recommended in January 1982, that Congress consider amending the disclosure provisions of the Internal Revenue Code to permit disclosure of SSA data on individual wages; net earnings from self-employment; and payments of retirement income to Federal, State, and local agencies administering Federal needs-based programs, whenever comparable data is not available at the State level.

One potential means of identifying income and assets unreported or underreported by applicants and recipients of needs-based programs is IRS records on taxpayer unearned income. However, exchange of these data is also prohibited by the Tax Reform Act of 1976.

IRS requires that data on taxpayer unearned income be reported through third-party information returns so that it can verify the accuracy of taxpayers' Federal tax returns. Third-party returns are submitted, for example, for pensions and annuities, interest income, dividends, lump-sum distributions from profit sharing and retirement plans, bearer certificates of deposit, and individual retirement accounts.

This information, which is maintained in the IRS' information return processing file, could be used to verify the unearned income being reported to the eligibility programs and, also, to indicate ownership and value of assets which produced the income.

A 1978 feasibility test done by the IRS for the SSA demonstrated the usefulness of information return data for identifying SSI recipients who receive interest income. The results, developed as aggregated data only, showed that 13.5 percent of the recipients did have bank account income. Further, based on the amount of that income, the SSA estimated that 2.5 percent of the 5,000 recipients owned more assets than allowed for SSI eligibility.

According to SSA projections, more than 100,000 recipients were potentially overpaid $122 million annually because of these unreported assets. The SSA concluded that matching of SSN's of all SSI recipients with IRS records and using the results to determine recipients' eligiblity appeared highly feasible and cost effective.

Given these results, and based on other work we had done in federally supported programs, we recommended in January 1982, that the disclosure provisions of the Internal Revenue Code be amended to permit disclosure of IRS data on sources and amounts of unearned income to Federal, State, and local agencies administering federally funded needs-based programs.

Both this and our previously mentioned recommendation on wage-related data recognized the need for restricting such disclosure so that tax return information would be made available only for purposes of, and to the extent necessary in, determining an individual's eligibility for benefits or the amount of benefits.

Because of privacy and other concerns, Congress has appropriately approached the opening of tax data with caution. In September of this year, Congress amended the Code to facilitate the disclosure of tax returns and return information for nontax criminal investigation purposes. The debates leading to this amendment, however, did not include the issue of using tax data to help administer needs-based programs.

While I am on the subject of privacy, I would like to comment briefly on the computer matching guidelines issued by the Office of Managment and Budget. These provide requirements that agencies should follow to comply with the Privacy Act.

We believe that the OMB guidelines are important because compliance with them would help assure uniform adherence with key provisions of the Privacy Act. In addition, the OMB guidelines add a requirement which is extremely important. The guidelines require agreements in writing with non-Federal entities that would not otherwise be subject to the disclosure controls of the Privacy Act.

These agreements should address such things as file ownership, limits on the use and disclosure of the files as well as the information extracted by the matches, and the nature of file disposition. Although these agreements are important, their implementation must be actively monitored by Federal agencies to assure compliance. We also believe that the guidelines can be improved by extending their coverage to computer matches that are aimed at verifying eligibility of persons before payments are made.

With regard to the requirement in the Privacy Act that calls for providing adequate safeguards over personal information, we have reported on a continuing number of computer security problems in Federal and State agencies.

Nonetheless, there are a number of recognized techniques and procedures which can be employed to give a high degree of computer security during a computer match. It is encumbent upon each agency to use these computer security techniques and procedures and monitor their use during the match to guard against unauthorized disclosure of personal information or other possible violations of the Privacy Act.

Mr. Chairman, to summarize our views, we believe that computer matching can be an effective tool for verifying the eligibility of entitlement program beneficiaries. However, such matches must be performed within the framework of the Privacy Act of 1974 and Tax Reform Act of 1976. Moreover, where legislation is needed in order to make additional data such as tax data available for matching and verification purposes, Congress must consider the privacy and tax compliance implications prior to authorizing or not authorizing the use of such data.

This concludes our prepared statement. We would be pleased to respond to any questions. Thank you.

Senator COHEN. Thank you very much, Mr. Campbell. Does the GAO believe that the Congress and/or the the OMB ought to approve each computer match that is proposed to be done using Federal data?

Mr. CAMPBELL. I guess the concern we have is with the word "approval." I think that that would create an administrative nightmare that nobody is prepared to deal with at the moment.

We would like to see maybe, in lieu of an approval process, some kind of a central focus or oversight role to insure coordination, compliance with standards, better control over Privacy Act considerations, those types of things.

Senator COHEN. What opportunity does Congress have for effective oversight? As you know, our oversight activities are fairly limited in their scope and ability to follow any particular piece of legislation or policy. Most of us have seven or eight or nine subcommittees. As you also know, the bells will be going off sometime soon this morning and I'll be off and running. In the meantime, the computer matches continue to go on.

How is Congress ever going to be fully aware of the kinds of things that are taking place which might very well constitute an infringement on privacy?

We spent some time yesterday talking about this. For example, the question of profiles, who sits down and figures out what kind of profile we're going to look at? Are we going to take all white males over the age of 40 earning more than $40,000 in southern Maine, for example, and compare that with recipients of welfare benefits or AFDC in New Hampshire?

I assume some profile could be drawn along those lines. And you can take each hypothetical and they could even become fairly hyperbolic, I assume. But where does the supervision or the oversight come into play in terms of controlling the types of ingenious profiles that can be drawn and that start going into the computer files?

Mr. CAMPBELL. OK, Mr. Chairman. Let me say first that, to my knowledge, none of the work that we've done in the GAO has involved the use of profiles. We have used identifiers for the purpose of making a quick initial screening.

The problem that you raise about oversight is the reason that I have some concern about the approval, because I agree that it's impossible for the Congress to rule on every request for a match that's going to take place in the Federal Government or, for that matter, in State government.

Senator COHEN. And OMB doesn't want the job.

Mr. CAMPBELL. And OMB—well, I haven't talked to them, but you're right—they probably don't want the job. But if there were a focus—and I'm not saying that OMB is the proper place for that to be—but if there were a focal point which would maintain some type of data base as to what's going on, provide some assurance to the Congress that the computer matches actually being done comply with certain standards, were properly justified——

Senator COHEN. Where are the standards?

Mr. CAMPBELL. There are some minimal standards for standardization put out by the Department of Commerce. We have recommendations. One of the problems we have dealt with is poor standardization. The data in the files, because it's not standardized, is incompatible. It's difficult to match. For example, names—a simple thing like a name. Last name first or first name first creates a real matching problem. One of those files has to be converted before it's compatible data.

We're pushing for standardization, for standards to be issued for making data more compatible in Federal programs. But if you had assurances that matches being performed within the Government were adequately justified on a case-by-case basis, conducted under the proper legal authority, with the proper controls built in, the right kind of security, matched for a given purpose, I think it would go further than what you've got today in terms of assurances about what's going on out there.

Senator COHEN. Right now we have virtually no control over the kind of matching taking place. That's correct, isn't it?

Mr. CAMPBELL. That's correct.

Senator COHEN. And we have virtually no standards as to what is going to comprise a proper standard for a computer match. And we have virtually no control over what types of profiles will be developed in order to put that computer matching list together.

And, in essence, we have no oversight by either OMB or Congress.

Mr. CAMPBELL. The only thing you have—OMB has certain guidelines as to what——

Senator **Cohen**. Let me tell you about the guidelines. The guidelines were changed in 1982. Now the guidelines say that there has to be notice published in the Federal Register, and not only that, but to notify Congress and OMB about the computer matches.

There was a match done on student loans back in August. That notice was not published in the Register until December. And yet, the OMB guidelines require a reasonable proximity of the notification to the computer match. I don't consider 4 or 5 months to be reasonable proximity.

Do you agree with that?

Mr. **Campbell**. Yes; I do.

Senator **Cohen**. So, in essence, what we've got is no system. We've got most of the agencies running loose with their own computer matches trying to ferret out fraud, waste, abuse—all of the things that we are holding oversight hearings on weekly to try and do. But the question is what sort of process do we use to get there?

I didn't mean to be facetious yesterday, when I suggested that having been a prosecutor and also a defense counsel, I came usually to the same conclusion: Most of the people that I was prosecuting and most of the people that I was defending were guilty. And yet, we don't abolish trial by jury; we don't abolish the appointment of counsel; we don't abolish all of the rights and privileges of forcing the Government to prove its case. That is because we insist upon a higher standard when the Government is acting against an individual citizen.

And I think we all agree to that.

So the question is whether we, because we're dealing in an area where people are turning to the Federal Government for assistance, neglect these types of standards? I was somewhat concerned about your statement that we ought to focus computer matching upon entitlement programs, because I think that is one of the basic concerns that many people have voiced about matching is the narrowness—not in terms of the dollars involved—but the narrowness of the focus in terms of what income groups we're looking at. Most tend to focus on low-income groups, for example, AFDC recipients, welfare recipients, and others who are applying for assistance to the Federal Government.

But, you see, in my judgment, there's a lot more money being wasted in a lot of the contracting firms doing business with the Government. And GAO, of course, has been very active in trying to put together proper standards or recommending proper standards for procurement practices, which until recently have been virtually nonexistence as well.

There's a lot of fraud and a lot of waste with companies which do business with the Federal Government and which get millions of dollars and have literally ripped off the Federal taxpayer. An example is the home health care program, with HCFA, which has no standards and no oversight and in which fraudulent groups being set up to get all of this money designed to help people stay in their own homes.

So one of the questions is: Are we too narrow in the focus of computer matching because we look solely at low-income people and those at the lower end of the spectrum?

I would think that you would want to expand that, wouldn't you?

Mr. **Campbell**. Yes, sir. I guess the reason for the needs-based programs—you've got certain eligiblity requirements that makes it very easy to match, like income, family size, those types of things. And those are easier to match.

I would like to make one comment. All the emphasis on computer matching seems to be on fraud for the purpose of catching the crooks and the cheats. But it's really a much more cost-effective tool than that. It's useful up front for determining eligibility requirements to see that the right types of people get into the right kinds of programs, as an internal control device for good management. It has a lot of uses and, unfortunately, when we talk about it, most of the time we talk about it in terms of trying to catch the crook or the cheat. Its application is pretty broad from a program management aspect, too.

Senator **Cohen**. And I appreciate that. What came out of the hearings yesterday was the sort of "double-edged sword" that's involved here, that, on the one hand, for example, computer matching is much less intrusive. One of the arguments made yesterday is that it's much less intrusive in terms of dealing with individuals. You don't have somebody stalking around or making a local call to your bank director, saying, can we have access to Bill Cohen's or Mr. Campbell's bank records?

But I find that to be a somewhat illusory type of argument because, on the one hand, while it's less intrusive, you also have less ability as a private citizen to know that somebody's looking through your records.

At least when a person appears at the bank directly, the director may very well place a call to you, or someone will notify you, a friend at the bank or whatever, whatever the situation might be. But when you're dealing with computer matches and the records happen to be down here in Washington, you have this big brain scan going on constantly. A good deal of private, confidential information is being rummaged through by this computer and you're unaware of it.

And that gets us into the questions about privacy and notice, and ability of an individual to correct erroneous information that is in the computer.

So it's not enough to say, "Well, it's a good internal control device." It's also a good device for helping people to have access to more Federal benefits by standardizing it. We can determine quickly whether a person qualifies under each individual program rather than the chaotic sort of patchwork that we have now.

By the same token, all of those benefits also have a downside. The downside is that you're losing, incrementally, at least, a good deal of your privacy. And those have to be balanced out.

Do you agree with that?

Mr. **Campbell**. Yes, sir.

Senator **Cohen**. Let's talk about the cost-effectiveness issue a little bit. Most of us tend to focus simply upon the dollars—you mentioned $10,000 to conduct a computer match which may save millions of dollars.

What about cost effectiveness? Should OMB or somebody determine the cost effectiveness before the computer match is done or after?

Mr. **Campbell**. As you know, the guidelines have been changed. It's our view that it's still encumbent upon each agency to carefully consider the benefits of doing a match on a case-by-case basis, weighed against the cost of doing that match.

One of the key elements there that is difficult to quantify is the deterrent value. One of the benefits that comes out of using this is the deterrent impact that it has. If it's generally known that Federal agencies are screening eligibility periodically by means of a computer match, that's a benefit that is tough to quantify. We think that it ought to be a factor and it's least considered.

Senator **Cohen**. We heard testimony yesterday that they have a large number of so-called hits that are determined by the computer match. But there are few successful prosecutions and even limited recoveries.

I guess the question is: Do you think that a good test is the raw hits, or the even solid hits, versus prosecution or versus recovery? Should that be the test of whether something is successful or unsuccessful?

Mr. **Campbell**. Well, this sort of gets back to the point that I was trying to make earlier: that is, prosecution is not the main purpose of doing one of these things. Most of the action that's been taken is to identify ineligible people who are improperly on the rolls and generally, the corrective action is to delete them and thus correct the situation from that point forward. Not very often do they attempt to get actual recoveries because of the nature of the program.

Senator **Cohen**. When you're talking about actual cost, do you take into account simply the $10,000 to get the matchup, or do you take into account the man-hours or people-hours involved in providing the verification that is necessary to make it effective?

Do you include the hours of verification as well and all the costs involved?

Mr. **Campbell**. Absolutely. The staff cost, the cost of the software package, the cost of running the package, the cost of purging the files. And let me say, too, that the computer match is only the first step. All it does is give you a very quick automated screening of potentials. The hard part is the manual. You still have to do the manual checking and verification to assure that you've got a valid hit.

Because of the quality of the data, your match may have a large number of raw hits, which may turn out not to stand the test when it comes to looking at the hard support.

Senator **Cohen**. In your statement, you indicate that data standards are a long-standing problem which makes it difficult to conduct a match. Why is that such a continuing problem?

Mr. **Campbell**. OK. I'm going to ask if some of my colleagues who have been working in the standards area would like to address that.

Mr. **Watts**. Well, one of the major problems in this area is that we do not have enough standards. But even with the few standards we do have, we also have a problem with people not complying with them. It requires a great deal of coordination among all the people, particularly when you're also dealing with State and local governments, to make sure that you're all doing it the same way.

And usually, we've seen within the Federal Government lack of a compliance mechanism to make sure that somebody is saying, yes, when we represent a date, we're going to show it this way all the time. We're going to show month, day and year, rather than year, month and day.

You have to have some sort of a compliance mechanism. Part of the other problem is that there has been, I think, a lack of appreciation on the part of top managers on the need to have standards. They look at it usually as an extra cost of doing business and something they don't have the time or the resources to put the money into. Let's just get the job done and move ahead. So a lot of times there's a lack of appreciation for the need for standards and also, I think, we just don't have a good compliance mechanism to make sure that the standards are, in fact, complied with.

Senator COHEN. You talk about computer security. What sort of problems are associated with computer security?

Mr. CAMPBELL. It's a real problem. And as the technology increases, the risk becomes greater, too. The problem, I think, is that computer security has had a relatively low priority. The low budget has been pushed down pretty far, organizationally. I think what we need to see is a greater focus on the part of the Federal agency—State agencies, too—on the security aspects.

Senator COHEN. Tell me about what the problems are.

Mr. CAMPBELL. Jim, would you like to address the specifics, there?

Mr. WATTS. Sure. Well, there's a variety of security techniques that can be used. But a lot of these techniques are people dependent. One of the key ways of preventing unauthorized access to a system is the use of passwords or PIN numbers, which you will have, for example, on some of your electronic fund transfer systems.

The problem is that you still must rely upon people to control their code words, the passwords, or PIN numbers. It's not infrequent that you can go into a computer room sometimes and see the code word taped up on a wall so the person won't forget it. Or we've also seen situations where people with EFT cards have actually taped their PIN number on their card. Well, if they lose that card, then whoever gets it can automatically get into that person's EFT account.

These are the kinds of things that we see. The other thing is that many of the security problems result from a lack of proper segregation of duties; that is, making sure that one person does only one part of the whole process and another person does the other part. But so many times we see the failure of people to maintain an adequate segregation of duties.

I'm familiar with some cases, for example, where an individual could get out of an automated insurance system, a policy premium refund check, and a policyholder cancellation notice. The individual then took the policyholder cancellation notices, tore them up, and went out and cashed the checks.

Well, those two things shouldn't come to the same person. There's a variety of things like this. There are good ways to prevent this, but many times we just don't have people in there monitoring to make sure that those controls are, in fact, working.

Senator COHEN. Have any standards or any guidelines been recommended by GAO for computer security?

Mr. WATTS. I think that we have pushed a great deal for the need for such standards. We don't have the authority within our agency to issue those kinds of standards. The National Bureau of Standards does and they have issued a number of guidelines and standards in the area for security.

Senator COHEN. Have you looked at those?

Mr. WATTS. Yes, we have looked a great deal at how the NBS has performed. And a lot of what they have come out with is very good. It's a matter of making sure that we have compliance with those standards and following through on the part of the people who are supposed to implement them.

Senator COHEN. In your assessment, are the standards adequate if they're complied with?

Mr. WATTS. I think so, for the most part. But as Will indicated, we have a moving train here with the technology. We have certain standards we have to put in place, but the technology is constantly changing. As that changes, we also have to have new standards that take care of that new technology.

Senator COHEN. I guess what I'm asking is whether the Bureau of Standards constantly updates their recommendations or do they pass them in 1972, and then we find ourselves in 1982 with outdated standards?

Mr. WATTS. Well, when we looked at it, they weren't doing a very good job of that. But now they do have a procedure where, I believe it's every 3 or 4 years, they have to go back and reevaluate a standard that they have put out to determine whether it's still valid, effective, or should we update it or come up with a new standard? That's the procedure that they have to comply with, and that's a common procedure in the standards area.

Senator COHEN. Do you think 4 years is adequate to keep up with a moving train?

Mr. WATTS. I think it is. But, you know, you have to monitor these things as you go along, and if something pops up, you have to take care of it. In other words, you have to work on an exception basis as well. I think that it's probably a reasonable length of time. Yes, I do. But it takes a long time to develop a standard.

Senator COHEN. And I agree, it probably does take a long time to develop a standard. But what about the sophistication of computer thieves? Do they take 4 years to figure out how to break a standard? [Laughter.]

Mr. WATTS. No; we have a lot of students today who could break systems rather easily. It's a challenge to them. My 12-year-old son, Jeff, works on an Apple computer at home. I'll tell you, he knows more about that doggone thing than I do. We have that kind of a situation coming up.

Senator COHEN. That's why I inquire as to whether 4 years is enough. When you've got the kind of geometric learning curve that's taking place—from an Apple I, then a couple of years to Apple III, and then maybe IV or V. Almost twice a year now you've got a new Apple machine coming out or some modification of another brand. And you've got students who are studying computer technology at the ages of 6 and 7 in school today.

Of course, with those who are going to pursue honest careers, there are those who are going to graduate with degrees in criminality as well. So I'm just asking whether 4 years is a reasonable time or should they be looking at it on a much more periodic basis, even though they can't issue the standards?

Mr. WATTS. I think the way it is set up is that they have to look at it every 4 years. That doesn't mean that they can't look at it earlier. I think that prudent management dictates periodic monitoring; and if a change earlier then 4 years is necessary, it should be done.

Senator COHEN. What does the GAO think of the efforts by the Veterans' Administration and by other agencies to obtain death data from private and State and other sources?

Mr. CAMPBELL. Yes, sir. The question of a national death file is one that's been kicked around and is being kicked around rather extensively. There's a lot going on in the Federal sector, as well as the private sector. The National Center for Health Statistics has a file. The SSA has a file. The Inspector General at the VA is attempting to put together a file. There are files available in the private sector.

We are presently taking a look at the whole question of a death file because there are a lot of questions that need to be answered about the quality of the data in the file. If you're going to have a national death file, do you need to have three or four agencies trying to develop one? If there should be only one national death file, who's going to maintain it, keep it up to date? That's got to be resolved. Are you going to sell it or is it going to be free? Who's going to use it? Who's going to have access?

There's just a number, a wide range of questions. We're undertaking a survey in one of our divisions to look at this whole question.

Senator COHEN. In some of the death matches that VA and OPM have performed, the Government files were actually given to a private company to match. Similarly, we're going to have some testimony later this morning about a bank match that was done in Massachusetts wherein the bank conducted the match.

So the question I have is, Should the Government send out its records to a non-Government entity for a match?

Mr. WATTS. I was going to say that the OMB guidelines allow that to be done. But there must be an agreement, a written agreement, between the Federal agency and the entity, to make sure that proper safeguards are established over what is going to be done with the hits, the disposition of the file, and how it's going to be safeguarded. I think, from our point of view, however, we want to do our work ourselves. We want to maintain that additional control over our own matches. We don't want to be sending our files out. That's pretty much how we've tried to approach it from an audit point of view.

Senator COHEN. Mr. Lainhart?

Mr. LAINHART. I think there's an issue here that we have tried to address in our office. As Jim indicated, we have taken the files and done the matches ourselves. We carried the files around with us in our automobiles, on airplanes, whatever, to not allow the data out of our presence. We have taken over computer systems and had them dedicated to just our job, so that no one else can access the computer system while we're using it.

I think your question is very valid, and needs to be addressed. I personally would not want to see it being done, and that's why our office has taken the position I outlined.

Senator COHEN. I think that a fundamental policy issue here is whether or not people who supply information to Government agencies are put on notice that that information that's supplied to the Government is going to be reviewed by personnel who are not Government employees, who are in the local community, who might use that information on a local basis, to their detriment.

All of those issues seem to have been ignored for some reason. There are provisions in the "catch-all" OMB guidelines which OMB doesn't even supervise. I have some real problems with allowing the private sector do the matches. It may be one thing to get information from the private sector, as we found out with the death facts they tried to accumulate. You may turn to a private company who might be creative enough to start developing its own files about who has died recently in the United States and supply that to the Government. But on the other hand, I don't think that the reverse should be true. I do not think that the Government should be turning over information to the private company to perform functions which are essentially governmental in nature.

Let me ask you whether or not Government records are sufficiently encrypted—I hate to use that word "encryption," since we're going to be dealing with it on the floor sometime later today. I guess it came to mind, Mr. Campbell, when you talked about the Seeker system. I wonder if that was any relative to the Peacekeeper. But I'll get to Seeker a little bit later.

Tell me about encryption. Do they encrypt records in order to prevent duplication by people in the private sector?

Mr. GLAGOLA. In our experience, the records that we have processed have not been encrypted.

Senator COHEN. Any recommendation that they should be?

Mr. GLAGOLA. Encryption during a match—actually, it would make it harder to do a match. You could encrypt the records on the front end, read the record in, decrypt it, do your match, encrypt it back, write it in encrypted format. But you're adding additional overhead to the matching job.

Senator COHEN. What sort of protection do you have against photocopying of records?

Mr. GLAGOLA. You can't photocopy electronic media.

Senator COHEN. OK. Can you copy? Can you duplicate the records?

Mr. GLAGOLA. Yes, you could duplicate them. However, you would have to be an extremely sophisticated person once copied to interpret a very complex master record ——

Senator COHEN. What if I want to hire Jim Watts' son?

Mr. GLAGOLA. Yes. [Laughter.]

A lot of the records that we deal with in the Federal Government are highly complex. They use coding techniques and record techniques which, if you are not familiar or you don't have what is commonly called a Data Elements Dictionary or a record layout, you would not be able to decipher the record.

Senator COHEN. Well, you know, I've been reading an awful lot of articles of how sophisticated crooks are becoming in our society. Over the years, this committee has held hearings dealing with how we educate our criminals in our prisons to duplicate social security cards. Any sort of identifying cards that we carry can be duplicated flawlessly. And they picked up that information in our prisons, where we trained them in various techniques.

I suspect that the same sort of criminal mentality is also evolving into the world of high technology. So that even though it's complex, it doesn't mean that there isn't going to be a sufficient element of people who are able to do that.

Mr. GLAGOLA. That is correct, Senator. The point I was trying to make is that the technology is evolving. People are learning the technology. But without the key, it makes it much more difficult.

Senator COHEN. Mr. Campbell, tell me about the Seeker system.

Mr. CAMPBELL. All right. Let me refer you to Mr. Glagola here on my staff, who actually developed the Seeker system for us.

Mr. GLAGOLA. Mr. Chairman, the Seeker system was originally developed in response to a congressional request from the Senate Finance Committee.

Senator COHEN. We don't always know what we're looking for or asking for. [Laughter.]

Mr. GLAGOLA. I just thought I'd throw that out as a little aside. Some of the things that the Senate Finance Committee wanted us to do when designing this system was to not rely on SSNS to perform a match and to take into account the quality of data when we did a match. And in addition, to try to take us a little bit farther down the road of the verification process. In other words, you had addressed earlier the problem of a lot of hits, but not much coming out. And when we designed the Seeker system, we tried to put some better techniques into it so that the hits coming out of the Seeker system would be of better quality.

It is designed as a general purpose system. It can be used for a number of different purposes. It has a specific record layout that you can place your data elements into and just run standard software to produce your matches.

It uses a weighted scoring technique. For instance, we would say that the SSN would have a weight of 40. And the last name may have a weight of 15. The weights are based upon the amount to which that particular data field would reduce the universe of potential matches.

By taking various combinations of the fields which matched between two individual records, we can come up with a score for that particular record and produce, in our estimation, a good quality match.

Senator COHEN. Do you have any plans to expand the capabilities of the Seeker system?

Mr. GLAGOLA. Yes, we do. We are currently in the process, or will shortly be, of adding information which would be relevant to the medical environment to do medical-type duplication process.

Senator COHEN. For example? What do you mean by that?

Mr. GLAGOLA. If a particular recipient had filed for a duplicate claim, had two blood tests done——

Senator Cohen. That would focus more upon the doctors, wouldn't it?

Mr. Glagola. Well, we intend to design it so that it can handle both sides, both the provider and the recipient.

Senator Cohen. One of the things that we found is one of the most flagrant abuses of our medicare-medicaid system is the overbilling or billing for services that were never rendered on the part of physicians. It is pretty flagrant—we had one physician who was in here who was so bad that he wanted to be caught. He was billing for hundreds of thousands of dollars. He actually—pathologically apparently—wanted to be detected, but only by chance did we pick it up. And that was because there was no oversight, no systems of control for that.

So that's what you're trying to pick up as well?

Mr. Glagola. Yes. We will build in various forms of variance that will allow differences from a standard. What's the term that they use? The reasonable cost from the built-in variance from what are the customary and reasonable cost factors so that we can select from various items.

Senator Cohen. That's all the questions we have for now. If we have others, we will submit them to you, Mr. Campbell, and ask you to respond in writing.

Thank you very much for appearing. We appreciate it.

Mr. Campbell. Thank you very much.

[Mr. Campbell's prepared statement follows:]

UNITED STATES GENERAL ACCOUNTING OFFICE

FOR RELEASE ON DELIVERY EXPECTED
AT 9:30 A.M., EST
THURSDAY, DECEMBER 16, 1982

STATEMENT OF

W. D. CAMPBELL

ACTING DIRECTOR, ACCOUNTING AND FINANCIAL
MANAGEMENT DIVISION

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT

SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

ON

COMPUTER MATCHING TO DETECT ERROR, WASTE, AND FRAUD IN GOVERNMENT PROGRAMS

Mr. Chairman and Members of the Subcommittee:

We are here today at your request to discuss the use of computer matching as a means for detecting and preventing error, waste, and fraud in Government programs. You asked us to present our views on whether computer matching is a cost effective management tool, and whether it can be used without compromising the privacy rights of individuals. You also asked us to address a number of specific issues, such as how often matches should be made, problems in performing them, and other benefits of computer matching.

Based upon our experiences as well as those of other agencies, we believe computer matching can be a very cost effective tool for detecting error and fraud in Government entitlement programs and for identifying actions needed to strengthen program controls. Even more important, as a form of internal control, it can be a very effective deterrent to fraud and waste if it is common knowledge that it is being used. Funding for entitlement programs is projected at over $350 billion for 1983, and potential erroneous payments could run into the billions. Because computer matching is a relatively low cost method of identifying and reducing erroneous payments, we endorse its use with the understanding that the rights of individual citizens will be protected as required by the Privacy Act of 1974, the Tax Reform Act of 1976, and due-process provisions for reducing or eliminating benefit payments are followed.

Definition of computer matching

Before I go any further, I think it would be useful to define computer matching and discuss briefly its use in entitlement programs. Simply stated, computer matching--as its name implies--is a technique in which selected data within a file or in two or more computerized files are compared to identify certain conditions which, if they exist, could indicate program ineligibility and erroneous payments. In the context of its use in entitlement programs, it is one step in the process of verifying eligibility information provided by people applying for or receiving program benefits. After a match has been made, additional steps must usually be taken to ensure that "matched records" pertain to the same individual and that the data in each record is accurate and up to date. Thus, because the computer provides the capability to match millions of records with extreme speed (vis-a-vis manual matching), computer matching is a systematic and efficient means of conducting a preliminary screening and matching of records to identify possible erroneous payments.

COST-EFFECTIVENESS OF COMPUTER MATCHING

For the most part, our efforts have focused on identifying erroneous payments rather than evaluating the cost-effective use of computer matching by Federal and State agencies. (See App. I for a list of reports related to computer matching.) Our experiences with computer matching have shown that the benefits--namely identifying and stopping erroneous payments and correcting program deficiencies--generally far outweigh the cost of a match.

As far back as 1976, for example, we made a computer match of Supplemental Security Income (SSI) payments with records of benefit payments made by the Veterans Administration and the Railroad Retirement Board. 1/ By using a computer matching technique, we were able to identify and report total erroneous payments of more than $60 million annually. The Social Security Administration has now been conducting similar matches routinely and we understand that in fiscal 1982 the savings actually exceeds $100 million.

We reported in January 1982 2/ that overpayments in 5 major needs-based benefit programs would probably exceed $1 billion in fiscal 1982. Since eligibility and the amount of these payments

---

1/Supplemental Security Income Payment Errors Can be Reduced," HRD-76-159, Nov. 18, 1976.

2/Legislative and Administrative Changes to Improve Verification of Welfare Recipients' Income and Assets Could Save Hundreds of Millions," HRD-82-9, Jan. 14, 1982.

are dependent on recipients' income and assets, increased verification of these data via computer matching could reduce significantly the number of erroneous payments. The estimate of overpayments was made for the AFDC, SSI, Medicaid, Food Stamp, and Section 8 Housing programs. Although significant, they represent only a portion of the total potential erroneous payments for all entitlement programs.

As you can see, the potential payback of a computer match can be significant, but the question remains: how much does it cost? The straight-forward answer is "it all depends" because there are so many variables. Costs will depend on such variable factors as the size and complexity of the records being matched, the quality and compatibility of the data in computerized files, and the extent of verification required following a match.

One element of cost is the cost of the software needed to make the match. This cost, by itself, can be large; however, once developed, the software can be used on many different matches. For example, our staff designed a set of computer programs for matching which we call "SEEKER"; our development costs were about $100,000. To date, we have used it on several different audits in GAO. Also, two executive agencies are using it now (the Veterans Administration and Department of Labor) and others are planning to. On one matching project alone we identified about $2 million in overpayments of which about $500,000 has been collected.

(Text)

Another element of cost is the cost of computer time to match the files, but, here again, the cost is relatively insignificant in relation to potential benefits. On a current audit, we spent less than $10,000 in computer time to match over four million records; the potential erroneous payments on the hits identified in the match may be several million dollars.

The remaining costs of a computer match are the most difficult to assess and these include the costs to review a match to confirm that an erroneous payment has been or may be made. This effort is usually manual and the costs are dependent upon the eligibility requirements of a given program and the quality and availability of data needed for verifying whether a match does in fact represent an erroneous payment. Consequently, it is difficult to generalize on these costs and each matching project must be evaluated on a case-by-case basis.

Operational problems increasing costs

Some major operational problems can further increase the costs and time involved in computer matching. They involve incompatibilities in ways data is represented in computer files of different agency systems and inaccurate and unreliable data contained in their automated files. We have addressed both of these problems in several reports and although some progress has been made, much more needs to be done.

We have reported the problem of data standardization in computers over the years. For instance, in 1974 we reported 1/ that the common coding and representation of information in computers was needed to facilitate exchanges of data in automated

---

1/"Emphasis Needed on Government's Efforts to Standardize Data Elements and Codes for Computer Systems," B-115369, May 16, 1974.

records in machine-readable form and reduce its cost. In 1978, we reemphasized the need for computer standardization to facilitate data exchanges and noted a lack of compliance with existing standards. 1/

As automated data exchanges become more prevalent for computer matching as well as for other reasons, the need for an effective approach to standardization becomes even more important for economy and efficiency reasons.

Another major problem that we have seen over the years involves poor data quality in automated systems. In computer matching, a major part of the cost involves validating the quality of the data in the files of the agencies involved in the match. Validation includes assuring that the matched data is complete, accurate, and timely. The more data errors in the files, the more it costs to validate the computer matches.

In addition to the added costs of performing a match, poor data quality can also result in the failure to identify improper payments being made. The added costs here are erroneous payments.

Factors to consider in matching

→ Because of the many variables involved, prudent program management requires that proposed matches be planned and properly justified and evaluated periodically in terms of costs and actual benefits. In assessing benefits, however, program managers both

---

1/"The Federal Information Processing Standards Program: Many Potential Benefits, Little Progress, and Many Problems," FGMSD-78-23, Apr. 19, 1978.

at the Federal and State level should view computer matching as a tool for preventing as well as detecting error and fraud and therefore its use can act as a deterrent to program abuse.

In this context, computer matching can be viewed as an internal control technique, as well as a tool for evaluating the effectiveness of other internal controls. For instance, computer matching can be used before benefits are authorized to validate or verify eligibility-related information provided by an applicant (e.g., wage data in needs-based programs). In this way, computer matching functions as an internal control to detect or prevent erroneous or fraudulent payments before they occur. Computer matching can also be used--very effectively as shown by its many uses to date--to determine if applicants already receiving benefits are truly eligible. In this way computer matching functions as a tool for determining if other internal controls used for verifying an applicant's eligibility for benefits are functioning properly.

COMPUTER MATCHING: WHEN AND HOW OFTEN?

→ With regard to your question of when and how often computer matching should take place, the issue centers around whether it should be done in the pre-payment stage or the post-payment stage, and if in the latter, how frequently?

Selective verification of critical eligibility factors through computer matching at the pre-payment stage would have the obvious benefits of identifying potential program abusers and errors before erroneous payments are made, reduce expensive followup and collection activities, and, as I stated previously, act as a deterrent in preventing or reducing the amount of program abuse that may take place. Consequently, matching at the pre-payment stage can be very desirable. It may not be feasible in all cases, however, because some programs may call for the initial payments to be made within a short timeframe. For example, the Food Stamp Act of 1977 (as amended) currently requires that allotments to eligible households be made in as short a period as 5 days, and not later than 30 days following the filing of an application. This requirement could make it difficult to use computer matches at the prepayment stage if the automated files to be matched are processed on incompatible systems or the data in the files is of questionable accuracy and requires significant amounts of verification before it can be used. If such constraints make computer matching impractical before initial payments or benefits are provided, consideration should be given to performing a match as soon as possible afterwards.

Because of changes in circumstances involving individual income, assets, dependencies, and the like, computer matches should also be considered for persons already receiving Federal benefits.

Whether matches should be performed, and whether the match should be on a one-time or routine basis are dependent on several factors and should be considered on a case-by-case basis. The obvious considerations are:

- --Specific known or suspected cases of fraud or error in a benefit program.
- --Whether computer matching would be effective in deterring people from misrepresenting information when applying for benefits.

- --Significant changes in legislative or administrative requirements for eligibility and payment. A match could be a very economical means for determining whether required changes were correctly made.
- --The potential for change in an individual's eligibility status. For example, changes in income or asset levels could change or eliminate eligibility for a benefit payment.
- --The adequacy of the system of internal controls in a benefit program. If controls are judged to be weak, a program could be more vulnerable to error or fraud. A more frequent match might therefore be in order until the controls are strengthened.

STATUTORY CONSTRAINTS TO COMPUTER MATCHING

While there are advantages to using computers to verify data about persons applying for or already receiving Federal benefits, the Tax Reform Act of 1976, which was designed to protect the privacy rights of taxpayers, restricts or prohibits the matching of certain computerized data.

In January 1982, we recommended 1/ some legislative changes to facilitate computer matching in needs-based benefit programs. In these programs an individual's eligibility is based upon his or her income and assets. Our recommendations addressed the use for verification purposes of (1) wage and earnings data maintained by the States and SSA, and (2) unearned income data maintained by the

---

1/Legislative and Administrative Changes to Improve Verification of Welfare Recipients Income and Assets Could Save Hundreds of Millions" HRD-82-9, Jan. 14, 1982.

Internal Revenue Service (IRS). However, the opening of Federal tax data for use in other government programs involves certain policy considerations concerning privacy.

Wage and earnings data

Wage data maintained by the States is generally considered to be the best available wage information for verification purposes. The States collect this information from employers to determine eligibility and benefits under the unemployment insurance program. However, there are a couple of limitations. First, only 38 States have laws that require collection of quarterly wage data for use in the unemployment insurance program. The other 12 do not; most get only gross payroll data from employers. The Department of Labor has recently drafted proposed legislation to respond to our recommendation to require all States to collect wage data quarterly.

Second, the data for all States does not include wages of Federal employees, military personnel, and earnings of the self-employed. SSA wage information is more comprehensive than State data because it does include these wages and earnings. A major problem, however, is that because these data are collected for Federal income tax purposes, as well as for SSA's use, access to the data is controlled, for privacy reasons, by the Tax Reform Act of 1976. This law was enacted to provide stringent disclosure limitations on tax return data because of concerns about individual privacy. Although the Congress has passed separate legislation making SSA's wage data available for use in the AFDC and Food Stamp programs, such data cannot be used for verification purposes in other Federal needs-based programs.

We recommended in January 1982 that Congress consider amending the disclosure provisions of the Internal Revenue Code to permit disclosure of SSA data on individual wages; net earnings from self employment; and payments of retirement income to Federal, State, and local agencies administering Federal needs-based programs whenever comparable data is not available at the State level.

Unearned income and asset data

One potential means of identifying income and assets unreported or underreported by applicants and recipients of needs-based programs is IRS records on taxpayer unearned income. However, exchange of these data is also prohibited by the Tax Reform Act of 1976.

IRS requires that data on taxpayer unearned income be reported through third-party information returns so that it can verify the accuracy of taxpayers' Federal tax returns. Third-party returns are submitted, for example, for pensions and annuities, interest income, dividends, lump-sum distributions from profit sharing and retirement plans, bearer certificates of deposit, and individual retirement accounts. This information, which is maintained in IRS' information return processing file, could be used to verify the unearned income being reported to the eligibility programs, and also to indicate ownership and value of assets which produced the income.

A 1978 feasibility test done by IRS for SSA demonstrated the usefulness of information return data for identifying SSI recipients who receive interest income. SSA provided IRS with the social security numbers (SSNs) of 5,000 SSI recipients who claimed to have no income from bank accounts. IRS then matched these SSN's against its files. The results, developed as aggregated data only, showed that 13.5 percent of the recipients did have bank account income. Further, based on the amount of that income, SSA estimated that 2.5 percent of the 5,000 recipients owned more assets than allowed for SSI eligibility.

According to SSA projections, more than 100,000 recipients were potentially overpaid $122 million annually because of these unreported assets. SSA concluded that matching the SSNs of all SSI recipients with IRS records and using the results to redetermine recipients' eligibility appeared highly feasible and cost effective.

Given these results, and based on other work we had done in federally supported programs, we recommended in January 1982 that the disclosure provisions of the Internal Revenue Code be amended to permit disclosure of IRS data on sources and amounts of unearned income to Federal, State, and local agencies administering federally funded needs-based programs. Both this and our previously mentioned recommendation on wage-related data recognized the need for restricting such disclosure so that tax return information would be made available only for purposes of, and to the extent necessary in, determining an individual's eligibility for benefits or the amount of benefits.

Privacy considerations and tax information

Because of privacy and other concerns, Congress has appropriately approached the opening of tax data with caution. In

September of this year, Congress amended the Code to facilitate the disclosure of tax returns and return information for nontax criminal investigation purposes. The debates leading to this amendment, however, did not include the issue of using tax data to help administer needs-based programs.

We continue to believe that this issue merits consideration. However, we recognize that the policy considerations are sensitive and complex. On the one hand, there are the tenets that taxpayers who supply IRS with tax information have a basic right to privacy with respect to that information, and that such information should be subject to disclosure only when society has a compelling interest which outweighs individual privacy concerns. Some believe that violation of these tenets might affect voluntary compliance with and, thereby, the health of the Nation's tax system. On the other hand, there is the need to improve needs-based program eligibility and benefit determinations so that benefit dollars are not lost to the Government or diverted from those entitled to them. We consider the problem sufficiently significant to warrant congressional debate and consideration.

THE PRIVACY ACT AND OMB GUIDELINES FOR COMPUTER MATCHING

While I am on the subject of privacy, I would like to comment briefly on the computer matching guidelines issued by the Office of Management and Budget (OMB). These provide requirements that agencies should follow to comply with the Privacy Act.

The Privacy Act of 1974 was passed because of concerns about possible invasions of the privacy of U.S. citizens by the Federal

Government. The Act requires agencies to issue public notices of the existence and uses of their "systems of records" containing information about people. It also specifies conditions under which personal data in these systems can be disclosed and requirements for maintaining records on such disclosures. Further, it defines the rights of individuals to obtain, review, and when, in error, amend records about them. Among other things, it also requires agencies to establish appropriate administrative, technical, and physical safeguards of records.

We believe that the OMB guidelines are important because compliance with them would help assure uniform adherence with key provisions of the Privacy Act. In addition, the OMB guidelines add a requirement which is extremely important. The guidelines require agreements in writing with non-Federal entities that would not otherwise be subject to the disclosure controls of the Privacy Act. These agreements should address such things as file ownership, limits on the use and disclosure of the files as well as the information extracted by the matches, and the nature of file disposition. Although these agreements are important, their implementation must be actively monitored by Federal agencies to assure compliance.

We also believe that the guidelines can be improved by extending their coverage to computer matches that are aimed at verifying eligibility of persons before payments are made. These types of matches are currently excluded from the guidelines.

With regard to the requirement in the Privacy Act that calls for providing adequate safeguards over personal information, we have reported on a continuing number of computer security problems in Federal and State agencies. / In a report entitled "Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" issued on January 23, 1979, we pointed out that ten Federal agencies were experiencing problems in establishing organizations, plans, procedures, and methodologies for cost effective computer security safeguards over automated data. In more recent reports issued in 1981 and 1982 we have found this to be a continuing problem in both Federal and State Governments because policy guidance has not been adequate and senior agency managers have given only limited support to improving agency security programs.

→ Nonetheless, there are a number of recognized techniques and procedures which can be employed to give a high degree of computer security during a computer match. It is incumbent upon each agency to use these computer security techniques and procedures and monitor their use during the match to guard against unauthorized disclosure of personal information or other possible violations of the Privacy Act.

Mr. Chairman, to summarize our views, we believe that computer matching can be an effective tool for verifying the eligibility of entitlement program beneficiaries. However, such matches must be performed within the framework of the Privacy Act of 1974 and Tax Reform Act of 1976. Moreover, where legislation is needed in order to make additional data such as tax data available for matching and verification purposes, Congress must consider the privacy and tax compliance implications prior to authorizing or not authorizing the use of such data.

This concludes our prepared statement. We would be pleased to respond to any questions. Thank you.

SELECTED GAO REPORTS FROM 1976 TO 1982 INVOLVING COMPUTER MATCHING

Report Title or Subject	Report Number	Date Issued
States' Capability to Prevent or Detect Multiple Participation in the Food Stamp Program	CED-82-103	06-16-82
Prisoners Receiving Social Security and Other Federal Retirement, Disability, and Education Benefits	HRD-82-43	07-22-82
Millions Could be Saved by Improving Integrity of the Food Stamp Program's Authorization-To-Participate System	CED-82-34	01-29-82
Legislative and Administrative Changes to Improve Verification of Welfare Recipients Income and Assets Could Save Hundreds of Millions	HRD-82-9	01-14-82
States' Efforts to Detect Duplicate Public Assistance Payments	HRD-81-133	09-17-81
Concerns About HHS' Ability to Effectively Implement Incentive Funding for State Information Systems in the Aid to Families With Dependent Children Program	HRD-81-119	06-29-81
Impact of State Death Information on Federal Income Security Programs	HRD-81-113	07-28-81
Millions Can be Saved by Identifying Supplemental Security Income Recipients Owning Too Many Assets	HRD-81-4	02-04-81
VA Improved Pension Program: Some Persons Get More Than They Should and Others Less	HRD-80-61	08-06-80
Social Security Should Obtain and Use State Data to Verify Benefits for All Its Programs	HRD-80-4	10-16-79

Report Title or Subject	Report Number	Date Issued
Social Security Student Benefits For Postsecondary Students Should be Discontinued	HRD-79-108	08-30-79
Social Security Should Improve Its Collection of Overpayments to Supplemental Security Income Recipients	HRD-79-21	01-16-79
Letter Report on Social Security Administration's Problems in Detecting Duplicate Payments Retirement, Survivors and Disability Insurance Program Benefits to Students	HRD-79-27	12-22-78
Letter Report on Duplicate AFDC Payments in New York	HRD-78-133	06-21-78
Wisconsin's Aid to Families With Dependent Children and Child Support Enforcement Programs Could Be Improved	HRD-78-130	06-22-78
Privacy Issues and Supplemental Security Income Benefits	HRD-77-110	11-15-77
Supplemental Security Income Payment Errors Can be Reduced	HRD-76-159	11-18-76

Senator COHEN. Our next witnesses will be State officials from New York and Massachusetts whose agencies have been actively engaged in matching for some time. First we're going to hear from Peter Wynn, the deputy commissioner for administration of the New York Department of Social Services. And then receive testimony from Mr. William Hogan, the secretary of the Massachusetts Executive Office of Human Services.

Mr. WYNN.

TESTIMONY OF PETER M. WYNN, DEPUTY COMMISSIONER FOR ADMINISTRATION, DEPARTMENT OF SOCIAL SERVICES, STATE OF NEW YORK

Mr. WYNN. Good morning, Mr. Chairman. My name is Peter Wynn. I'm deputy commissioner for administration of the New York State Department of Social Services. In my official capacity, I am responsible for the audit and quality control and fraud and abuse activities of our department, for the finances of the department, for the budget of the department, and for a variety of other housekeeping chores.

My comments this morning are going to be quite informal. I have submitted some testimony. I would like, if I could, to dwell on a half dozen different points that seem of interest to us, and I would think perhaps of interest to you.

We at the State level administer most of the public benefit programs that we have been talking about here in the last day or two. And we find ourselves in a schizophrenic setting that I would like to describe. For example, much of the driving force behind our efforts to perform tape matches and for computerization of the welfare program comes from congressional and administration demands that we achieve error rates that are, we think, virtually unachievable, and that if we do not achieve these error rates, we will be sanctioned. So, on the one hand, we are being driven and pressed and pushed and compelled and subjected to huge possible sanctions, and on the other we feel that we are not often given the tools and the wherewithal or even the freedom to use the tools and the wherewithal we have to manage our programs better.

So that's the setting in which we took off as early as 1977 with a whole series of computer matches and of computer development. And I thought it might be of interest for me to describe briefly the first large match effort we performed, which was in New York City with medicaid providers. I'm not talking about recipients; I'm talking about high-income doctors, institutions, hospitals, clinics, medicaid mills, methadone providers, doctors, in some instances, who are pulling hundreds of thousands of dollars down out of the system.

We were able to take 7 years of New York City medicaid payment tapes. The city had simply kept a record of payment of a bill paid and had not performed any serious effort at manipulating that data to insure that duplicate payments were not made.

This is all well known, but it's not well known in the context of tape matches. And I don't mean to disparage the city's efforts. That was a huge undertaking. We had 170 million transactions contained on 20,000 reels of tape. In 1977, we received from our State legislature an appropriation to create a medicaid fraud and abuse unit, which we did. That consisted of almost 300 people. We took the tapes, wrote computer programs, and began to look for evidence of abuse, evidence of misuse, and mispayment. And in the course of that, discovered that medicaid mills, which had been legislated out of existence, had gone underground. We learned that the medicaid mills, for example, had simply gone underground and that doctors and dentists and pharmacies and other providers would simply bounce a patient, a recipient, from one to the other to the other.

We discovered when we compared payments made on behalf of a given recipient, we would find that on a given day, we had paid five providers for services rendered that recipient, indicating clearly a bouncing of the recipient from one provider to another. Sometimes, of course, that's appropriate. Other times it's not.

In any event, through this mammoth effort, we were able to recover tens of millions of dollars in misspent medicaid funds, in duplicate claims paid to institutions, often, again, not a purposeful attempt on the part of a clinic to seek duplicate payment, but the payment system was so tardy and frankly, not subjected to the kinds of edits that we ultimately subjected the system to, that bills would be paid twice, often 6 months late, but they would be paid twice.

In any event, through this effort, we believe we have significantly and perhaps even largely cut medicaid provider fraud out of New York City, and we now have in place state-wide the medicaid management information system which performs over 400 edits on incoming claims before they are paid. This has been a huge saving. We have estimated 5 percent of our medicaid budget has been saved through implementing this system.

Let me go back to the second large system that we have in place in New York, and that's the welfare management system. This was legislated at the same time as the MMIS, the medicaid system, and was, and is, designed as a recipient eligibility file. It enables us to retain on our data base the recipients of service and the kinds of service to which they're eligible. We have 5,000 terminals and printers around the State of New York in each of the welfare offices, and upon presentation of an applicant, the data is captured in a workbook. The data is then transmitted to our computer to determine if the recipient is known to us from another county, for example, which enables us for the first time to insure we don't have recipients applying from many counties, adjacent counties.

We also compute the benefits to which the recipient is eligible at our central site, and that information is telecommunicated back to the county offices. We can do such things as mass rebudgeting. When the Congress, for example, changes the benefits, we can compute all of that centrally in a matter of hours, instead of taking days, weeks, and months at the county level.

We are tying these systems together. The welfare management system produces the recipient eligibility file that is used to make the medicaid payments. And, candidly, we are seeking to tie more of our systems together so that we have a comprehensive systems base to: First, better manage our program; second, keep the costs down; and third, provide recipients better service. And incidentally, the output of this is files that can be used—and we are using—to control the integrity of our program.

That takes me to our third system: the wage reporting system, about which I believe you've heard something already. The wage reporting system was legislated in 1978. We implemented it. It's been in place now 4½ years. We believe that it is cost effective. I understand that there was some discussion of this yesterday. Let me make a few points.

It's been suggested that the true costs to the State, the true returns to the State, are overstated. I would say that that's not the case. We believe we have conservatively saved—we will save $30 million this year. Those savings are primarily computed on the AFDC program. We have not yet even counted in the savings resulting from the quick-turnaround system, which I would like to digress to describe.

We now have in place in New York City the following process. If an applicant comes to any one of the 40 income maintenance centers, it ordinarily takes a week before eligibility is finally determined. At the first interview, basic data is obviously captured. The name and social security number are taken at each income maintenance centers, accumulated at the end of the day, sent to the New York City computer center, put on a tape, and telecommunicated to us in the evening. We take the tape to the wage reporting system in the department of Taxation and run the applicants of that day against the wage reporting file, pull off any instances where wages were reported, and send that data back via telecommunication to New York City—where it's put out to the income maintenance centers on their screen at the start of business the following day.

We have found that the availability of this data, even though it is dated, is an extremely useful tool in the interviewing process, in that it gives the interviewer, the eligibility worker, a piece of data that can be explored.

We have found, and our next annual report, I believe, will show that 2 percent of the applicants for assistance in New York City have been correctly denied because of the availability of wage data which was not divulged by the recipient at the time of application.

That is a very significant saving. That translates into $20 million, roughly. We haven't included that saving as yet. We have not included the savings attributable to the location of absent parents which come about through utilizing the wage reporting system.

Senator COHEN. I'm going to have to interrupt you and declare a recess for about 10 minutes so that I can go over and vote and come back.

[Recess.]

Senator COHEN. Mr. Wynn, in case you didn't know, that's a 10-minute vote by congressional standards. [Laughter.]

I was hoping to catch a vote at 11, and then because of the last amendment having passed, they decided that they will not take up the 11 vote until some indeterminant time, which is probably 5 minutes from now and we'll have to recess again.

So with that in mind, why don't you just proceed?

Mr. WYNN. Fine. I was commenting on the wage reporting system and our view of its success, which I gather wasn't shared by everybody yesterday. We think that the wage reporting system is providing savings in excess of what we have reported to date, that is, $30 million expected this year. We think it's much higher. We can defend that, and we will do so. I will be sending something to your committee.

Second, it has been alleged that the costs of running a program such as wage reporting are higher than we have reported. That, too, is not the case. We have a budget bureau. We have a legislature that oversees our expenditures and appropriates money for the purposes for which it was intended. And we have expended only those funds that we have shown in our annual report.

There is a point to be made, however, that when we do a wage report run against the employer records, against our AFDC rolls, we prepare a mail-out document on each recipient where there have been assets or earnings in excess of what would be expected. And that is sent on a computer-prepared form with a turnaround document directly to the county. The county is responsible for following up on investigating that situation where there are unreported earnings. And they are responsible for taking the appropriate action, that is, either reducing the benefits or removing the person from the eligibility rolls.

There is a turnaround document that comes back to us. My audit and quality control people oversee the effectiveness of that operation. There is a cost involved at the county level of pursuing these now computer-generated instances of earnings.

This is, however, highly efficient. These people are out in the counties, in any event, investigating what heretofore were allegations—telephone allegations, anonymous allegations, or whatever—of misuse of the welfare system.

That is a very, very inefficient way of going after fraud—chasing down anonymous phone calls or letters or whatever. Now we are able to target the efforts of these program integrity folks much more carefully and much more pointedly and, frankly, we think much less onerously from the point of view of individual rights and individual privacy.

The cost to the employers—it's been suggested that the costs to employers of reporting the wages quarterly is not taken fully into account. I would only say that at the sunshine hearings about 1½ ago, we had the major employer professional associations in New York as part of the hearings. And while there's always a certain amount of grousing about having to report anything to the Government, as we're all aware, the employers, by and large, acknowledged that the benefits of this system, to society as a whole and to them as corporate and private taxpayers, far outweighed any problems they had with the reporting process itself. Many of them have now switched to magnetic input and felt that that was inexpensive and highly efficient. And we also offered to investigate the possibility of changing the format of the file from the concept of every employer reporting every employee quarterly to every employer reporting only a change in employee status. We're not sure that's the way to go, and I don't think that the employers are, either. But we're certainly looking into it as a response to a suggestion by the Empire State employers.

And finally, the idea here that there are more effective methods—more effective methods of investigating and pursuing recipient fraud—just does not hold water. That is a highly labor-intensive process, unless you have some means of targeting your efforts. And that's precisely what the wage reporting system provides.

We now have in my audit control division about 850 people—which is, I might point out, just slightly smaller than the HHS Inspector General's operation. We used to have a little over 1,000. And the reason for that was that we didn't have the targeting tools that modern technology have provided us, such as the MMIS, the wage reporting, and the welfare management system. We've actually cut our manpower input into this and increased our efficiency.

Finally, on that subject, we view matches—tape matches and computer matches—as one of the many tools that we used in our audit and quality control operation. And every significant effort we undertake, whether it's reviewing the determinations at the county level that a given recipient should be home relief, and we go in and find that it should be AFDC—that's a project that we've recently done, which, frankly switches State expenditures to Federal expenditures. It saves our State money.

Every project such as this—every project such as wage reporting or vital statistics reporting, all of these projects are analyzed for their cost/benefit ratio. And we rarely undertake a project with less than a 5-to-1 cost/benefit ratio, which is very low. Usually we look for 10 to l, or even more. That's done all the time. We're sometimes wrong.

Senator **Cohen**. How would you know that? If you're looking for a 5 to 1 or 10 to 1, how would you know that up front?

Mr. WYNN. We don't know it often up front. What we try to do most of the time is take a sample, take 500 cases, take 100, do a probe sample, then follow up with a statistical sample and try to analyze what the universe is, what the payback will be, what the costs will be. That whole process is an art, admittedly, and we're often wrong. But we try to do it, and we try to do it as realistically as we can. The primary tool is the sample, frankly. We do a sample. Sometimes a blind sample.

For example, we wanted to know whether the New York State Department of Taxation refund file and dollar amounts would justify us seeking to run our absent parent with delinquent child support payments, court-adjudicated delinquencies, would produce a return. So we took a 500-case sample of 4-D cases where there was an absent parent where the court had said payments are due, and where the payments were in arrears. We ran that blind against the refund file of the taxation department. That is to say, we gave the names. The taxation department did the run and came back with a statistical report, not an individual report. And we found that the payback for that would be 20 to 1. Then we sought State legislation and got it, and we now have a New York State Taxation Department intercept program for arrearages in the 4-D program. That's the kind of thing we try to do.

I only have a few more comments, and then I would be more than happy to answer questions.

I think one of the problems that we have in this whole area of computer match is the appearance of secrecy. I think we need to dispell that. Even if it isn't an attempt at secrecy, that's the way it looks to the public. I think we need to tell people very, very clearly what it is we're doing—what file goes where, what is spun against what, who does what? Maybe even in—I don't want to say comic book, but in a very, very simple, easy-to-understand form so that people know what we're doing instead of suspect what we're doing. I think they suspect of us a lot of things that simply aren't there.

And second, we need to have—others have said this, too, and I would just second it again—we need to have a means of letting people who feel that they have become a victim of tape matches, a means for them to rectify any mistakes, to correct an error, to make sure that their rights ultimately are honored and that an error is not perpetuated.

Let's see if I have any—oh, I wanted to mention a point here. We have done vital statistic matches in New York recently. That is death matches. And here's an example of what could happen to you.

We did a match of medicaid providers against the deaths of that year—1981, I believe it was. Here, again, we were looking for providers. This is not recipient fraud; this is provider fraud. And we got back—I've forgotten the number—but a significant number of hits where a provider was still enrolled in a medicaid program, but he had died. And we thought, oh, my heavens. What happened here? We had several hundred. It was a significant number.

We investigated and found that in only six instances had any payments been made for a claim by a provider who had died prior to the claim. So that several hundred shrank to six. We looked at the six, and we found only two where there was any fraud. The other four, it was a pharmacy and the provider—the surviving spouse, who was also a pharmacist, had not changed the provider number, things like that.

Sometimes you run against situations where there is no payoff, and we just drop it. Now we may continue to do vital statistic matches on recipients, and I think perhaps the SSI program should, but we're not going to focus on providers any more.

The other point I wanted to make is because you mentioned it, and that is the idea of having a private enterprise utilize government data in matching. I think that was in relation to the death match, was it not?

Senator COHEN. Yes.

Mr. WYNN. I think it really depends. You'll hear shortly from Massachusetts, where——

Senator COHEN. We had information in another hearing on Monday which dealt with a private firm supplying death data to the Federal Government. But the situation I'm referring to, and I assume will be testified to this morning, is where the State of Massachusetts had a bank do the actual matching of bank records.

Mr. WYNN. Yes, I would like to speak to that. I think that that has to be looked at on a case-by-case basis or on an industry-by-industry basis or whatever, because I would far rather have us supply recipient social security numbers and perhaps the first three digits of their last name, or whatever, some basic data, to a bank and have the bank do the match and tell me when we found a case of concealed assets or suspected concealed assets than have the bank give me a list of 1 million depositors, of which only 1,000 are my recipients and the other 999,000 are people who I have no interest in whatsoever.

So that I really think you have to look at that from both sides. We, for example, in the wage reporting system, have the Department of Taxation do the actual match. We don't do it. We don't take the tax records or the wage records into our department and do the match and expose data on people who have absolutely no business being in our department to people who work in our department. That's really all I have immediately on my mind, although I can certainly talk about this stuff forever. It's fascinating.

Senator COHEN. Unfortunately, we've got about 3 minutes before the bells go off again, and I have to leave. You indicated in your written statement that people who seek public assistance must relinquish some degree of their rights to confidentiality. Do you think that that applies to anybody who does business with the Federal Government or the State government?

Mr. WYNN. It is very hard to get a really generalized position on this. It seems to me that there are only two totally defensible positions: one is you refuse all access to all records for any purpose to which they were not intended. And the other is you open everything up and say, let's look at the tax records. Let's look at everything. Let's match——

Senator COHEN. What do you think?

Mr. WYNN. Neither one of those extremes is a position that I want to take. So I'm left somewhere in the middle. And as I tried to describe, I think not particularly eloquently, it seems to me that if a sector of our society, quite appropriately, gets some kind of preference in terms of tax dollars in terms of public funds, for their personal sustenance and use of medical care and all of those things that I believe in——

Senator COHEN. Farmers?

Mr. WYNN. Sure.

Senator COHEN. Small businessmen?

Mr. WYNN. You lead me down the path and at some point, I have to say no.

Senator COHEN. You see, the point is when you say that some segment that gets public assistance, well, they're all out there. Everybody's getting public assistance. Every single element in our society gets some form of public assistance, whether it's a doctor getting reimbursement from medicaid, whether it's a farmer seeking some sort of wheat program or sugarcane program, whether it's small business looking for some sort of assistance through the SBA. There isn't anybody out there who isn't part of this "Federal Government." They're all sharing in the tax system.

Mr. WYNN. You point out the obvious problem that I face, too. I don't know the answer to it. I do think that in my case the realities of trying to make our system work, with all of the pressures on it, and I include those that your body puts upon us, lead me to believe that I have to use those tools. And I'm able to rationalize it in my mind that these people are getting a very direct preferential position in the disbursement of money, even though it may be miniscule compared to the profits of Lockheed, or whatever.

I don't have any good answer for you, Senator. I really don't.

Senator COHEN. Mr. Wynn, I particularly appreciate your candor and also having the benefit of your testimony. I thought your opening statement about the schizophrenic atmosphere in which you have to function was particularly relevant. I can understand that because I am part of your problem.

Congress, from time to time—quite a bit of the time, as a matter of fact—does mandate programs or policies or insists that we're going to clean up all the fraud, waste and abuse in our government. And we pass laws and then suddenly we say, well, wait a minute. It's a bit more complicated than that. We really shouldn't be only looking at fraud, waste and mismanagement. We also have to look at rights, because certainly you have a much more, I assume, efficient collection of information in the Soviet Union than you do in the United States, with everybody feeding into Big Brother in the Soviet Union.

So the question becomes whether you have policy tradeoffs—to what extent will you go to become efficient if you sacrifice the very things that you believe separate you and make you special in the ways of the world?

So that's something that we don't always think about in advance. We do it and then we think about it later and then we have to have oversight hearings and say, "Where are we going?" But it does create a heck of a problem for you when we do mandate that you have, as you put it, reduced your error rates to unachievable levels.

Mr. WYNN. I might also comment that I hadn't heard much reference to it in the several hours that I've been sitting here, but we have a State legislature and we have a populace and pressure groups and everything that we are as big as—we are the ninth largest industrial power in the world. And we have all the powers and pressures and tools that you have. And believe me, our State legislature oversees us with an incredible scrutiny. Every piece of matching legislation that we have sought—in most of our big systems, we have had to seek an appropriation and legislation—have contained in them specific privacy requirements.

For example, when asked by Tom McBride and Dick Kusserow to match our wage reporting data against the federal workman's compensation rolls, we had to say no because our State law wouldn't let us.

So please keep in mind that there is a great deal of oversight going on at the State level, and this may have a very direct bearing on how involved you at the national level want to get in this.

Senator COHEN. There's very little going on at the Federal level, virtually none.

Mr. WYNN. I gathered that from listening this morning.

Senator COHEN. Thank you, Mr. Wynn.

[Mr. Wynn's prepared statement follows:]

TESTIMONY

Presented by

Peter M. Wynn

Before the
Senate Subcommittee on Oversight of Government Management

December 16, 1982

Mr. Chairman and distinguished members of the Senate Subcommittee on Oversight of Government Management, I am Peter M. Wynn, Deputy Commissioner for Administration of the New York State Department of Social Services which is the "SINGLE STATE AGENCY" responsible for the administration of the programs of AID TO FAMILIES OF DEPENDENT CHILDREN, (Title IV), MEDICAL ASSISTANCE, (Title XVI), SOCIAL SERVICES (Title XX), and FOOD STAMPS within New York State.

The annual budget of our Department is approximately 12 billion dollars, and we provide assistance of some kind to over 2 million New York State citizens annually.

I was pleased to receive an invitation to testify at your hearing today. It gives me an opportunity to impart a New York State perspective to the subject of your deliberations as I will be speaking about our experiences in using computer matching techniques to enhance social welfare program integrity. But before I address this subject, I believe it would be appropriate for me to share with you some recent history concerning the progress we have made in reducing program error rates in New York State.

I must emphasize that we have been extremely active in seeking ways in which to enhance the integrity of our assistance programs. And, we have achieved a considerable degree of success. Illustrative of the progress we have made is that in the past ten years, the rate of payment error in our AFDC program has been reduced from 26% to 7%, or by more than two-thirds. An explanation of how we have done this would consume too much of your time to be warranted, but suffice to say that our various corrective action efforts range from very simplistic procedural steps to highly sophisticated computer systems.

These systems include a statewide Welfare Management System (WMS), which now encompasses over 5,000 terminals and printers located in welfare offices throughout the State (except New York City, where implementation is underway) all connected to our Albany central computer for real-time interaction with our central data base; the Medicaid Management Information System (MMIS), which processed 80 million Medicaid claims annually in an average of 10 days, against over 400 system edits; the Wage Reporting System (WRS), which matches quarterly assistance program recipients against employer reported earnings - more about this system later; and a myriad of other systems covering Child Welfare, Child Support Enforcement payments, Fair Hearings, etc. The objectives of these systems are to detect and prevent errors before they occur, permit efficient and cost-effective management of these huge programs, and provide better and more humane service to our clients. An ancillary, but very real benefit, is that these systems produce the computer files which allow for inexpensive, highly automated tape matches. These tools are equal of almost any management device available in the private sector.

New York State has made a major commitment to error reduction and we have achieved progress in that direction. But, we are not satisfied with the present state of affairs. Indeed we stand squarely with Congress in our desire to reach the lowest possible error rate in our assistance programs. We are, however, entirely opposed to the use of the Federally mandated, but State operated Quality Control Programs (QC) as the tool with which to levy financial sanctions against the States. Such misuse of Quality Control not only destroys the utility of AC as a management tool, but is not a fair or even-handed device for apportioning sanctions across the country. Consider, for example, the position in which I find myself: I am responsible in the NYS Department of Social Services for both the Quality Control Program and the finances of the Department. I am being asked to not only fall on my sword, but to forge the sword as well.

The following is a listing of computer file matches currently conducted in New York State.

1. WMS Integrity Match -

   With the WMS implemented in the 57 New York State Counties, coupled with New York City Interim Recipient Eligibility File, we are able to insure that no recipient can file for benefits from more than one county.

2. Wage Reporting System -

   In cooperation with the NYS Tax Department - daily, monthly and quarterly matches are performed against the wage data base. The universe of clients matched range from new applicants thru absent parents with wage data available current and historical up to 7 quarters. Cost to run this system is 6 million/year with estimated savings of 32 million/year.

3. Unemployment Benefits -

In cooperation with the NYS Department of Labor - monthly client files containing Public Assistance recipients over age 16 are compared against the UIB master file and matches reported to NYS DSS for recovery action. Cost associated with this match is approximately $12,000 annually with savings of $463,000 annually.

4. State Payroll -

Monthly matches are performed against the NYS payroll and public assistance files, identifying matches. Cost associated with this match is minimal (less than $5,000) with annual savings of $30,000.

5. Bendex -

Monthly public assistance client change data is submitted to SSA for SSI and SSA and federal earnings match. There is no federal cost associated with this and estimated annual savings are $650,000.

6. Vital Statistics -

Periodically, in cooperation with NYS Bureau of Vital Statistics, NYS DSS client provider files are matched to determine deceased individuals who are shown as active clients. The cost and savings involved are minimal, however, the presence of this match has a very definite deterrent value.

7. NYS Blue Cross -

In cooperation with the NYS Blue Cross - a match is performed using the NYS DSS client file. Annual costs incurred is $12,000 with actual dollar recoveries of $650,000 and cost avoidance estimated at 2-3 million.

8. Bank Resources -

Currently a pilot project operated by Nassau County matching Nassau clients with 36 banks. Cost estimates are minimal and projected annual savings are conservatively 1 million.

9. New York - New Jersey Duplicate Assistance -

This project, done annually, matched all NYC cases with New Jersey for possible duplicate assistance. Cost estimates are minimal and annual saving is $65,000.

The following matches have been proposed and are in various stages of development or consideration:

1. NYS Department of Taxation Name and Address file to seek social secruity number of absent parent to use in locating an absent parent for child support.
2. NYS Department of Taxation Delinquent Absent Parent Refund to effect an intercept of any tax refund payment to offset deliquent support payments.
3. Interstate Wage Reporting to enable us to check across state lines for unreported earnings.

4. On-line NYS Motor Vehicle files to assist in absent parent location.

5. Recipient eligibility file against grantees of Educational Opportunity Program Grants.

6. Assistance recipients against Workman's Compensation roles.

7. Assistance recipients against benefits paid to retired or disabled military personnel.

8. Assistance recipients against Federal Payroll Files.

9. Assistance recipients against payroll and benefits of active military personnel.

We in New York State are acutely aware of the implications of computer matching processes to fundamental rights of privacy and confidentiality. In my own mind, I have resolved this conflict in the following way. Recipients of social welfare benefits are receiving preferential treatment in the disposition of public funds, and quite rightly so, in my view. In order to insure prudent stewardship of these public funds, and to establish recipients preferential rights to a share of these funds, recipients must relinquish some of their rights to confidentiality. I would hope that your debates on this issue will focus on how the non-recipient of social program benefits can be protected from incursion into their privacy. I firmly believe reasonable measures by government to verify information used to allocate funds to recipients of benefits must be supported by Congress; any other stance is clearly counter to recent clear Congressional priorities on error reduction in public benefit programs.

Thank you for your attention.

Senator COHEN. We'll have to declare a recess before we go to Mr. Hogan to testify, and I will try, if at all possible, to be back in that 10-minute timeframe, assuming that we don't have another vote to follow right away.

We'll stand adjourned for 10 minutes.

[Recess.]

Senator COHEN. The committee will come to order.

Mr. Hogan, why don't you proceed, and we'd appreciate it if you could summarize your statement since the bells may go off again.

TESTIMONY OF WILLIAM T. HOGAN, SECRETARY, EXECUTIVE OFFICE OF HUMAN SERVICES, STATE OF MASSACHUSETTS, ACCOMPANIED BY THOMAS H. SPIRITO, COMMISSIONER; HENRY A. CRETELLA, GENERAL COUNSEL; JOHN F. CASSEDY, DIRECTOR, SYSTEMS AND OPERATIONS, MASSACHUSETTS DEPARTMENT OF PUBLIC WELFARE; AND KERMIT C. MORRISSEY, DIRECTOR, EXTERNAL AFFAIRS, EXECUTIVE OFFICE OF HUMAN SERVICES, STATE OF MASSACHUSETTS

Mr. HOGAN. OK. Thank you very much, Mr. Chairman, and I thank you for the opportunity to testify on a subject of great importance, not only to the Federal Government, but to State governments and to recipients.

I think Peter Wynn summarized it quite well. We do have safeguards and oversight by our Massachusetts Legislature, by advocacy groups, and by others. I think what I would like to add to that is that in this time of very limited resources, we must be vigilant and make sure that only those eligible receive assistance, or the alternative is to reduce the benefit level, which I think is not acceptable at this time.

We began a rather comprehensive management improvement program in welfare in 1979 in Massachusetts and the bank deposit match is only one of our initiatives.

We changed our policy. We made the policy much clearer, and we structured worker discretion. We put together a competent legal staff. We automated many of our systems. Unemployment compensation benefits and earned wages were matched with welfare recipients, as provided by the law. Child support enforcement was strongly supported and encouraged. We improved our audit and quality control and the bank deposit match was the other initiative that we have taken, and with some rather dramatic results.

Verification of assets for public welfare recipients in Massachusetts was authorized by State statute in 1967 as part of the enabling act transferring welfare from the towns and cities to State government. And Massachusetts law provides financial penalties for noncompliance. But we really needed other initiatives to make the plan work.

Banks were reluctant initially to threaten their relationship with customers, and Massachusetts law requests data only for those who receive benefits. The department of public welfare provides banks with names and social security numbers of recipients and banks make the computer runs.

In addition, we set up a task force of legal, program, and computer personnel to visit with the various Massachusetts banking organizations to explain the purpose and to solicit their cooperation. An explanatory letter was sent to the treasurers of all the banks and the credit unions in Massachusetts. It was absolutely essential that we get their cooperation to make the program successful.

The process begins with the request from the commissioner of the department of public welfare to a bank or group of banks to match welfare lists with deposit accounts. The banks then return the computer list with a mark opposite those welfare recipients holding bank assets and the amount of the asset. The list is then sent to the State computer center, where a series of edit checks are performed to validate the file. The system sorts the matched records by category of aid, AFDC, medicaid, general relief, food stamps, and SSI to determine those cases which have liquid assets in excess of the eligibility standard for each of the categories.

The department of public welfare then sends termination notices to excess asset cases, and they are also referred to the bureau of special investigations for fraud inquiry. That particular department is not under my secretariat.

The department of public welfare legal division files complaints in the courts and freezes the assets in each account for the amount previously paid in benefits. The SSI cases are referred to the Social Security Administration for appropriate action.

Now we've taken several safeguards to prevent as much as possible an invasion of the rights of privacy of individuals. In the first place, for six quarters prior to the time that we initiated this bank deposit match, we sent a notice with the check to every welfare recipient that we were going to be initiating this match. That's 18 months' prior notice to everyone who was receiving welfare.

Senator COHEN. What does the notice say?

Mr. HOGAN. It said that we were going to be verifying their assets by means of a bank match, the bank deposit match. Also, one of the first things I did as commissioner of public welfare was to take the rights and responsibilities statement, which was the last part of the application form, and make sure that it became the first—on the first page of the application form. I saw no sense in having it at the end. So that now the workers are trained—they make sure that the recipient understands their rights and responsibilities. We also say that we're going to verify the assets.

And as Peter Wynn said, the undisclosed assets was our major cause of error, which precipitated our action to do something about it.

We also set the standard for the bank match at $500 above the eligibility standard. We did that so that if the bank match came on a particular day when someone deposited his or her check, if we kept it at that lower level, it might indicate that there were excess assets. So what we do is we set it at $500 above that to take care of that particular problem.

As a further safeguard, because we had some errors on the social security numbers, especially, we changed the situation now so that we use the social security numbers and the first letters in the last names. And this has cut down the errors insofar as the use of social security numbers in identifying the particular person.

Senator COHEN. How much has it cut it down?

Mr. HOGAN. I think it went from 24 to 7, if my recollection is correct.

Senator COHEN. Twenty-four what?

Mr. HOGAN. Twenty-four percent to about 7 percent. Also, the recipients who received termination notices are notified of their right to appeal and to continue receiving benefits pending a welfare referee's decision. Two phone numbers are also provided to provide the recipients and their legal representatives consistent and helpful answers to their questions about bank matches. And actually, nearly 1,000 phone calls have been answered through the use of these phones.

On the cost of the match—the cost to the State for the bank match consists largely of added legal staff in the department of public welfare and the apparent future needs for added staff in the bureau of special investigations as a result of the increase in volume that we have sent over to them.

We estimate that the added annual cost to the State is about $400,000. On the costs to the Massachusetts banks, for banks with in-house computer capacity, the cost is estimated at about $3.50 per 1,000 deposit accounts in the bank. For smaller banks which utilize service bureaus for computer runs, the charge is $5 per 1,000 deposit accounts.

The costs to the banks, then, is a function of scope of service and the resulting number of accounts that they have. As a result of the bank match, we estimate the following savings. We have completed matches with 117 banks. This is approximately 12 percent of the 1,013 banks in Massachusetts. We have gone through about 7 million accounts. Within this sample, there are now 2,224 cases identified with bank assets that make them ineligible for benefits. If all Massachusetts banks were matched, the department of public welfare estimates a conservative potential savings of about $110 million—$40 million in annual caseload savings and $70 million in recovery of funds previously paid.

Senator COHEN. Let me just stop you a minute. You said $40 million in caseload savings. Do you assume that's in perpetuity if a person is above the requirement and then is taken off? Whatever benefits he might be receiving from the State, does that mean that they are not going to go back on?

Mr. HOGAN. No. We estimate—we set it for about 1 year that they wouldn't come back on. That was a projection based on the amount of assets they had that we found that would make them continue to be ineligible for a period of probably up to a year.

Senator COHEN. One year?

Mr. HOGAN. Yes. The preliminary data that has not received a final edit indicates that more than 1,600 Massachusetts recipients, as a result of our bank match, 1,600 recipients may hold bank assets in excess of $5,000. Eleven recipients may have more than $100,000. And one may have $228,572. That was the largest one that we have found. Forty-five recipients may have assets of $50,000 to $100,000. And 169 may have assets from $25,000 to $50,000.

Senator COHEN. That's out of the total of 224 cases?

Mr. HOGAN. 2,224.

Senator COHEN. The ones that you mentioned before, the ones that said—you had 224 cases that were identified as being ineligible for continued receipt of benefits. Then you gave me those examples there.

Mr. HOGAN. I'm sorry, Mr. Chairman. If I said that, I meant 2,224 cases.

Senator COHEN. 2,000?

Mr. HOGAN. Identified with bank assets make them ineligible for benefits.

Senator COHEN. I'm sorry.

Mr. HOGAN. The confidentiality of public records has not been at issue in Massachusetts. We published our intent to verify assets at the time of application, and the applicant signs with full knowledge of that. It's explained to them that we're going to do this.

Under social security numbers——

Senator COHEN. Can I ask you a question?

Mr. HOGAN. Sure.

Senator COHEN. Has that served as a deterrent, in your judgment? One of the lines of testimony that has been coming through in the last couple of days is that computer matching, as long as people are aware of it, will serve as a deterrent, so that if people know in advance that their bank records are going to be checked or matched against their welfare identification number, or whatever, that that will deter them from taking advantage of it. And once that's been announced publicly, that you have people calling up saying, "Take me off."

Did the prior notice 18 months ago, or whenever it was started, serve as a deterrent to take people off, in your judgment?

Mr. HOGAN. In my judgment, it did. Our caseload in Massachusetts has gone down since 1979 from a total of 123,000 AFDC cases. As of yesterday, the caseload in Massachusetts was 90,600. Part of that was changes in the Federal eligibility. There's no question about that. But I think that definitely, this has had—the fact that we are notifying people and there has been some publicity on the fact that we are going to be verifying assets I think definitely has had a deterrent effect.

Senator COHEN. I have been reading articles about the reindustrialization of Massachusetts, about Massachusetts coming back from a very low period of employment and now rebuilding with new technology coming into the State and thereby having a much brighter promise for jobs.

Would that not equally be persuasive as a factor, that you've got a better economic climate and therefore lower welfare rolls?

Mr. HOGAN. Absolutely. There's no question about that. I think that there are other factors, and I didn't mean to exclude others.

Senator COHEN. I just wondered how you determine whether it serves as a deterrent as opposed to a better economic climate.

Mr. HOGAN. The better economic climate is definitely a factor. I think our work and training program is a very definite factor. I think our efforts in child support—of the cases that have been removed from the welfare rolls, and that's thousands and thousands of them, we did a study and only 11 percent have returned to the rolls.

I think the reason that you stated, the economic vitality and the climate in Massachusetts, is one factor. The work and training program is the other factor. And the increase in child support gives a person who was originally on welfare just enough additional income so they don't return to the rolls.

I think that all of those factors are important. I think that there is definitely a deterrent effect.

Senator COHEN. Is there another factor, which I won't ask you to comment on, but is there another factor, such as the political climate in a given State that, for example, if you go through a period of liberalism, as such, with a Governor and suddenly you have a radical change in government in the State of Massachusetts over the past 3 or 4 years, with crackdowns announced on welfare cheats and abusers and suddenly, you have a shift in your welfare rolls?

Does that have an impact, in your judgment?

Mr. HOGAN. It certainly does.

Senator COHEN. And now you may have a different—notwithstanding your computer matches, you might have a shift back. With a different Governor and to a more liberal state of mind and a more charitable way of dealing with people, you might have a reversal of that, notwithstanding the computer matches; right?

Mr. HOGAN. I wouldn't expect that it would——

Senator COHEN. Well, if one could have a negative impact, can't another one have a positive?

Mr. HOGAN. Oh, I think so. I think the fact of the matter is that even though the welfare rolls were reduced significantly, the benefit level was increased in the last 4 years by 16 percent. So I think that there are all kinds of factors. Political factors are definitely very important, and I don't think that any reform like this could take place without the total commitment of the Governor and his policies.

I didn't have anything further to add. Commissioner Spirito is here, the commissioner of welfare. I think I would like to point out that I have read some material on *Lesade* v. *Spirito,* and I do want to point out for the record that a petition for a temporary restraining order was brought in the district of Massachusetts. It was not granted. They didn't meet the burden. So that the first hurdle has been overcome insofar as the bank deposit match is concerned. A temporary restraining order was not granted.

Senator COHEN. Was there a petition for a complaint for permanent injunction now?

Mr. HOGAN. The case is dormant at the present time. There has been no movement in some period of time.

Senator COHEN. Tell me about your appeals rate under this system. What has been your experience?

Mr. HOGAN. I would like to ask the General Counsel, if he would, he would probably give you a clearer picture, if you have no objection.

Mr. CRETELLA. The appeals rate has been higher than for any other program that we have. Approximately a little less than 50 percent have appealed our termination letters. And of those appeals, approximately a little less than half have been upheld. The reason for the upholding of the appeals, the additional information furnished by recipients to show, for instance, that there was a trust, irrevocable trust, in existence, which is not apparent from the deposit information itself.

Senator **Cohen**. I'm going to stop you right there. Isn't that one of the problems in terms of verification? Wouldn't it be better to verify first whether or not it was a trust account as opposed to putting it through the list and matching it up and say, you're over the $500 limit and above the eligibility requirements and bingo, we've got, not a "raw hit," but a "solid hit," and therefore, we put the burden on you to appeal the case. A termination notice is sent, bank assets are frozen, and they're up on appeal and now they've got to go forward. And usually, these people are low-income individuals who don't have immediate access to attorneys. Most attorneys aren't willing to take those cases; frankly, there's no money in them. So they have to go to some sort of public assistance law firm. In the meantime, they come back and say, well, we didn't make a mistake. It's just that you had a qualifying factor on which we're in error. We didn't check that out and therefore, you're back in now.

Don't you think it would be a fairer system to say that you, the State, have the burden of at least verifying that before you force them to go to an appellate proceeding?

Mr. **Cretella**. That was, of course, part of the claim in the *Lesade* case, that our procedures required——

Senator **Cohen**. Forget about the legal requirements. I'm not talking about that. I don't even want to pass judgment on that. I'm asking you as a matter of just a policy of fairness, who should bear the burden of those kinds of proceedings?

Mr. **Cretella**. We weren't free to act in a vacuum and treat the matter as one where we could make that kind of decision. Back in 1979, in our initial wage match, we were sued by Legal Services because we did precisely what you're talking about. We called the people in and attempted to ascertain what had happened. We were retrained from continuing that type of approach because the court, in the claim by Legal Services and the court's decision, took the view that we were actually investigating a criminal matter in the guise of determining eligibility for welfare assistance.

And the terms of that restraining order required us to separate very carefully our administrative process from the investigative process. We were prohibited from asking the type of question that you're suggesting right now.

In determining our approach for the bank match, we decided that we should not run the risk of having that type of claim made once again, particularly in view of the fact that we were under that restraining order. And we determined that it was probably more appropriate to handle it completely administratively on the basis of the information that we got and what edits we were able to employ without contacting the recipient. And then there is some inconvenience to the recipient, obviously. But if they had a legitimate claim, it would be upheld and maintained in our appellate process, in the complaint for judicial review process, just as in any other case of a recipient differing with us on our evaluations.

Senator **Cohen**. Let me just be clear on this. Suppose you had your hit that you matched up and you said that this person is over by $500, or whatever. And you sent out a notice to that individual that, according to your guidelines and according to the rules and regulations and the laws of the State of Massachusetts, that they are, therefore, in your judgment, to be termed ineligible. And that you further say if we are in error in this regard, you should plan to contact our administrative side of the agency to correct whatever error we're suffering from.

That would be prohibited under the existing restraining order?

Mr. CRETELLA. No. As a matter of fact, we do exactly that, Mr. Chairman. They are given information as to a telephone number that they can call, explain the situation, and we have, under those circumstances, undertaken to verify the information that they have given us.

For instance, Secretary Hogan mentioned that there was a problem with social security numbers initially. When we received that information by phone call, we undertook to go back to the banks and have that specific account verified. And when we determined that there was, in fact, an error, we terminated the action.

Senator COHEN. Tell me, if that's the procedure, then why do these people get reversed on appeal? Why were their cases on appeal reversed by them producing that information?

Mr. CRETELLA. Well, we have made another determination that it would be impossible to determine the legal nature of their claim of trust over the telephone. We have asked them to submit that appeal and to submit that information in the appeal process so we can look at the instrument or the hearing officer can look at the instrument and make a determination that there is a valid trust or not.

One of the things we have found is that there are many claims of trust, but very few that are actually legitimate, irrevocable trust that we are able to say is not available. Most of the trusts are what we call bank trusts. A person will open up an account in his name in trust for his son or daughter, or her son or daughter. And those are not valid trusts. The asset is considered available for purposes of our program.

And it's that type of thing that we're unable to ascertain without seeing what the documents are.

Senator COHEN. And if you request them to bring the documentation in, are you in violation of the restraining order?

Mr. HOGAN. The restraining order does not apply particularly to the bank match, but I think the claim would be that we are violating the spirit of that restraining order if we were to ask them to come in to explain something that existed in the past.

Senator COHEN. So if anybody's got a trust, then they are automatically geared into the appellate process.

Mr. CRETELLA. Yes, unless they have disclosed it already. And there have been some instances, very few, where the disclosure was made at the local office level and it did not come through at the central office level. And when that was discovered, of course, we terminated our action at the central office level.

Senator COHEN. Has there been any extension or broadening of this matching in Massachusetts to include contractors or student loans or other groups of individuals who are not on welfare or benefit of public assistance?

Mr. HOGAN. I have no knowledge of any matches. I think that we have been using it—well, I know that we have been using it for third-party reimbursement on the medicaid side.

Senator COHEN. You need specific authorization from your legislature to do that?

Mr. HOGAN. I do not believe so.

Senator COHEN. Our prior witness from New York of course indicated that they have fairly strict oversight and supervision, so that they are required to seek legislative authorization. But you are not required to—if you want to broaden it, for example, to start dealing with white collar crimes as opposed to welfare cheating or fraud. Would you be able to do that without having legislative authority or oversight?

Mr. HOGAN. I would not want to do that without legislative authority.

Senator COHEN. So if you intended to do computer matches in your State, then you go to the Governor, to the legislature, and you say, this is what we intend to do and we want you, No. 1, to be on notice and No. 2, to approve it?

Mr. HOGAN. Yes. I think if you look at the record in Massachusetts, this year the number of bills that have been passed, especially the long arm statutes for child support and things like that—so that if we do want to adopt any program, we go the legislative route.

Senator COHEN. Let me come back to the joint bank account or the trust account. What about those cases where people set up accounts for their burial expenses? How would you pick that up in your computer match?

Mr. CRETELLA. We wouldn't, is the short answer to your question, Mr. Chairman. Again, that would be the type of thing where we'd have to look at the documentation. These have come up outside the context of a computer match and they are usually referred in to our office, the central office, legal office, to determine whether or not they are irrevocable.

Again, the test if irrevocability and you have to examine the terms of the burial contract or the arrangements that the person has made to determine whether it's an available asset or not.

We have made this kind of ruling, both within the context of the bank match and outside that context since I've been associated with the office.

Senator COHEN. As I understand it, when you have the bank match, does the bank do the matching or do you do the matching?

Mr. CRETELLA. The bank actually does the matching against their accounts. However, it's placed on our tape. The mechanics are that we furnish a tape containing information that we have in our recipient master file, which is the social security number and the name of the recipient. They will run that tape through the appropriate software programing against their account tape, and where there is a match, the information is transferred to our tape. The tape is returned and then we do the printing of the information in our central computer facility.

Senator COHEN. What sort of arrangement do you have with banks in Massachusetts in terms of maintaining confidentiality of records?

Mr. HOGAN. The same laws which—the privacy statute in Massachusetts applies to anyone to whom the information is disseminated. So that they would be liable for suit civilly and prosecuted criminally for disclosure.

Senator COHEN. What kind of penalties are involved in the Massachusetts law?

Mr. HOGAN. I'm not that familiar with it.

Mr. CRETELLA. They're not extreme criminal penalties. The personal liability, of course, would be the invasion of privacy and whatever you would name as your damages in a civil suit would be the measure of damages.

Senator COHEN. Well, you weren't here yesterday, but one witness indicated that the Privacy Act—and we're going to hear some testimony shortly from an expert in the privacy law field—has been rendered obsolete by the use of computer matching. No. 1, you've got to show that you suffered physical harm or damage. As I recall, you've got to show a willful violation. You've got the excuse or the rationale used that it's a routine use of the information. So, for all practical purposes, no remedy.

Mr. CRETELLA. I don't believe that to be true. Even employees of the State in Massachusetts, under the Massachusetts privacy statute, are liable as any tort fees, or would-be unwarranted disclosure of information they receive. The banks are informed when the tape is furnished to them that under the statute, they become holders of that information and subject to the same restraints and liabilities if they were to make an unauthorized disclosure.

I don't know of any limitation on the right of action that an injured person would have to seek damages. I don't know whether there would be a criminal prosecution in every case, but there seems to be ample vindication of their personal rights through the civil action process, without limitation, subject to a showing of damages, of course, and the willfulness, and so forth, the unauthorized nature of the disclosure.

Senator COHEN. Just a couple of quick questions. Mr. Hogan, what about the amount of money spent in appealing these cases? Do you have a substantial amount of money devoted for going to the appellate level for the appeals process? Is that factored into your cost effectiveness with matching?

Mr. HOGAN. My understanding is that it is.

Senator COHEN. There seems to be an inordinately high amount of appeals with respect to other types of administrative cases. You talk about 50 percent, less than 50 percent, half of which are successful on appeal. The reason I am a little bit sensitive about this is that we've been going through some extensive hearings on the whole issue of social security disability cases. And again, we have the same sort of conflicting goals; namely, we want to take people off of the disability rolls who don't belong on there. By the same token, you want to keep people on who do belong on there.

The difficulty has erupted because of the mandate from Congress. We're the ones who mandated the overview on our disability program because GAO said 20 percent of the people on disability don't belong on there. Consistent with your statement, Mr. Hogan, if you don't start just paying the money to people who deserve it, there's going to be less money for those that do.

So we've to get those off the rolls.

But the problem that has come about is that we have devised a system which relies principally upon computers. Because of the effort being made to throw out the people who don't belong on the disability rolls, you've got terminations taking place with no human contact. You've got a very significant amount of appeals taking place, with about 50 percent of the cases being appealed and two-thirds of those cases that are appealed are being reversed because of information that those individuals were, in fact, entitled to disability.

The problem is that it takes between 12 and 18 months to have an administrative law judge hear a case. And those people who are desperately in need of hope go 18 months without that help, only to be told later on, "We're sorry, we made a mistake. You are in a body cast, and we didn't realize that, or you are in an iron lung, and so forth, and we should have known that before."

But that's the reason why I ask about that 50-percent appellate rate. Half of those 50 percent are being reversed.

Mr. **Spirito**. Mr. Chairman, I'd like to point out one important ingredient to this. Fifty percent of those people who receive notices did not request an appeal, 50 percent. Eighty percent of those people who did, in fact, appeal continued to receive aid.

Senator **Cohen**. Yes. I was going to say that sometimes there's a reason why people don't appeal. You're dealing with people in the lowest income level of our society. They are not always the best informed about legal rights, for example, or they don't have access to attorneys. They may feel that there is no sense in fighting city hall, and therefore they don't take advantage of the appellate route. There are a lot of reasons why they don't appeal—not simply that they're satisfied with the case. But I recognize what you're saying.

Mr. **Spirito**. The appeal is really inquisitory.

Senator **Cohen**. OK. In other words, you're saying you continue the payments during the period of appeal?

Mr. **Cretella**. Yes.

Mr. **Hogan**. Definitely. May I comment on the SSI disability? I think there are two criteria.

Senator **Cohen**. But you freeze the assets in the bank during the appellate process; is that right? So that you would have access to overpayments.

Mr. **Spirito**. Right.

Senator **Cohen**. I'm sorry. Mr. Hogan?

Mr. **Hogan**. I was going to say that we've been plagued with that problem statewide. And it seems to me that the agency requirements are different from the criteria used by the administrative law judge. The administrative law judge is using the——

Senator **Cohen**. The Constitution.

Mr. **Hogan**. Exactly. And there's no connection between the Code of Federal Regulations and the criteria that's being used at the local level. And I don't know how you just can continue that with that situation.

Senator **Cohen**. Let me tell you what's going to happen. Not this year, but believe it or not we're almost through over there. At least by January 2 we have to be through. But I assume that as soon as the next session starts, we're going to try and develop a comprehensive bill to deal with this problem of different standards.

What you have, in essence, is administrative law judges applying the law, which is what they are duty bound to do. And that means the Constitution. It means court cases. It means a body of law that has developed.

What you have within the administration, however, is a policy determination saying that from now on there will be no pain taken into account. You cannot at that case level take pain into account as a disabling factor, when, in fact, pain is part of the standard that we have written into the law. It says that it shall, if it's supported by reasonable medical evidence, be a factor in determining whether you're disabled. And yet, the administration determined that we're putting too much emphasis on pain. Cut it out. It doesn't exist. And here's a notice sent to every single local office saying, not to consider it any more.

So it's no wonder we've got a different rule by ALJ's as opposed to the social security disability offices. We're trying to correct that. But in the meantime, we're trying—I'm pleased to hear what you have to say—to see to it that the payments are continued, at least to the administrative law judge level. When you're talking about a couple of hundred thousand people who would otherwise be wrongfully dealt with, you shouldn't shift that burden on them during that appellate process, to somehow make it through.

That isn't fair, I don't think.

So what we're trying to do in the meantime is continue the payments. That is what you're doing in Massachusetts, which I commend you for.

Mr. Cretella. If I may, Mr. Chairman, I'd like to point out one thing—that our appeal process is not nearly as long as the social security appeal process. The appeals have been handled with existing staff. They have maintained adherence to our standard of a decision within 30 days. So it's a relatively prompt process.

Senator Cohen. Well, if we have more questions, I will submit them to you in writing and request that you supply the information as soon as possible. And I thank all of you for coming and testifying.

Mr. Hogan. Thank you, Mr. Chairman.

[Mr. Hogan's prepared statement with attachments follow:]

TESTIMONY OF SECRETARY WILLIAM T. HOGAN, JR.
MASSACHUSETTS EXECUTIVE OFFICE OF HUMAN SERVICES
BEFORE THE U.S. SENATE SUB-COMMITTEE
ON THE OVERSIGHT OF GOVERNMENT MANAGEMENT

December 16, 1982

Mr. Chairman and members of the Committee, I thank you for the opportunity to testify today on a subject of great current importance to the federal and state governments. Federal laws and Massachusetts law relating to welfare require that payment of public benefits be made only to eligible applicants; and that public funds not be spent on applicants or recipients who are not eligible.

Massachusetts initiated a comprehensive management improvement and modernization program in the Department of Public Welfare following the election of Governor Edward J. King in 1978. In 1980, I was appointed Commissioner of Public Welfare to implement the improvement program. I was elevated to the position of Secretary of Human Services in July, 1981, and succeeded by Commissioner Thomas H. Spirito. Together, we have continued the initiatives already begun. A summary of the progress made is attached to testimony I am submitting to the Committee today and I need not comment further on the results at this time.

I will briefly summarize the major steps taken which made possible the progress in Massachusetts welfare administration.

A planned sequence of initiatives was implemented as follows: clear agency policy was developed and applied to operations with equally clear structuring of worker's discretion; a dedicated and competent legal staff was assembled; automation was raised to the highest priority; unemployment compensation benefits and reported wages were matched with welfare recipients as provided by Massachusetts law; child support enforcement was strongly supported (Massachusetts and Wisconsin now lead the nation in child support effectiveness); audit and quality control activities were substantially increased; and emphasis was placed in the field rather than the Central Office. All of these initiatives have contributed, directly or indirectly, to the success of the Massachusetts anti-fraud program.

It should be emphasized that the verification of assets of welfare recipients does not, by itself, constitute an adequate agenda for reducing waste and fraud in public benefit programs. Rather, it is an effective tool in a comprehensive effort to improve and modernize welfare management. A well managed public welfare agency is, by definition, one that prevents and deters waste and fraud in every phase of its operation and one that provides benefits to eligible recipients in a timely, efficient manner.

Welfare fraud potential is not confined to recipients of benefits; the Massachusetts Department of Public Welfare has also improved its post-audit and recoupment functions and has recovered significant sums of money improperly paid to Medicaid and other service providers.

It is also necessary to note that while fraud prevention is more desirable than fraud detection, this choice is not always available to Departments. The dependence on manual processes at the state level, the incremental development of many of the welfare administrative processes and the incremental development of laws and regulations has created unanticipated policy loopholes and forced departments to focus on fraud detection, not merely fraud prevention.

Verification of assets for welfare recipients was authorized in 1967 as part of the enabling legislation that transferred welfare responsibilities from the cities and towns of Massachusetts to the State government. Amendments and added provisions in subsequent years authorized the matching of unemployment compensation benefits and wages with the Massachusetts welfare caseload. In 1978, interest income was added to the match list. (Copies of the relevant Massachusetts statutes and a list of all the computer matches currently used by the Department are attached to the end of my testimony.)

While the 1967 statute provided the Department with the authority to request account information from banks, and established financial penalties for banks that refused to comply, additional initiatives were necessary to assure the cooperation of the banks. Banks are prohibited by the Federal Privacy Act from disclosing personal information and are reluctant to take actions which might threaten their fiduciary relationship with their customers. Thus, the enabling statute was designed to permit the Welfare Department to request account information only for individuals who are "charges" upon the Commonwealth, and to further insure that the privacy of financial information is protected, the Department provides the banks with a tape of recipient names and social security numbers and the banks perform the actual computer runs.

Another step was taken to assure banks and banking personnel that the goals of a bank match initiative were compatible with their responsibility to their clients. A task force of legal, program, and data processing personnel was assembled to visit the various banking associations, explain the benefits of the program, and solicit the bank's cooperation. The Department also sent letters explaining the mechanism of a bank match system to the treasurers of all banks and credit unions. The cooperative relationship established between banking service institutions, the commissioner of banks, and the state Welfare Department proved to be critical for Massachusetts' success with the bank match initiative.

The results of the first match of bank deposits were announced early in September, 1982, and the results of two additional tests were made public on September 22, 1982.

The consolidated results of the three tests have been widely disseminated and I will focus my remarks upon the bank match process to highlight developments and respond to the specific concerns of the Committee.

The bank match process originates with a request from the Massachusetts Department of Public Welfare to a bank or group of banks, to match the names and social security numbers of welfare recipients against their deposit account records. The banks then produce a tape of welfare recipients by social security numbers holding assets in the bank and the amount of these assets. This tape is forwarded to our data processing center where it is entered into the Bank Match System, and a series of edit checks are performed to validate the file. The system then sorts the matched records by category of assistance to determine those cases which have liquid assets in excess of eligibility standards for specific benefit programs, such as Medicaid, AFDC, Refugee Assistance, General Relief, SSI, and Food Stamps.

When the Department finds a case that has excess assets, a termination notice is sent and the case is referred to the Bureau of Special Investigation who research the amount of time that the case had extra assets in the bank. The Bureau of Special Investigations is the agency that is responsible for fraud investigation in Massachusetts. Simultaneously, when appropriate, the Department's legal division files a complaint with the courts to freeze the assets in each account for the amount of benefits previously paid by the Department to the case.

In addition to these steps, the Department has added a number of precautionary measures to ensure that the process of bank matches does not infringe on the constitutional rights of welfare recipients. For example, the asset limit criteria used to determine instances of fraud is set approximately five hundred dollars above the program eligibility limits. This buffer ensures that cases which have just deposited a welfare, pension, or social security check will not be penalized by the snapshot approach of the bank match. To safeguard against wrongful terminations of assistance, the latest computer runs match a recipient's social security number in addition to the first two letters of the last name to avoid mistakes that resulted from erroneous social security numbers. The Department projects that bank matches which use these dual edits are approximately 93% accurate. Similarly all recipients who receive termination letters are notified by the Department of their right to appeal and to continue to receive aid pending a welfare referee's decision. And finally, two specific phone numbers are provided so that local offices, recipients, and their legal representatives may receive consistent and helpful answers to their questions about bank matches. Department records show that nearly 1,000 individuals have already made use of these phone lines.

The main cost to the Massachusetts Department of Public Welfare for the bank match is in the need for added personnel to investigate and prosecute cases suspected of fraud. Additional legal staff is needed to process the cases in the Massachusetts Courts. And the Bureau of Special Investigations has indicated a need for added staff because of the large volume of bank match cases being referred to that agency.

The cost of the bank match program to the participating banks is estimated at $3.50 per 1,000 deposit accounts if the bank uses its existing in-house computer capacity. Where a service bureau provides the computer capacity, as for smaller banks, the cost to the bank is $5.00 per 1,000 deposit accounts. For example, if a large bank with its own computer capacity has 1 million accounts, the cost would be $3,500.00. The cost to banks, then, varies with the number of deposit accounts in different size banks. A bank with 2 million deposit accounts would mean a cost of $7,000 to run the Massachusetts welfare cases against its accounts.

The Department has now completed computer matches against the records of 117 banks, or 12% of the 1013 banks in Massachusetts. If the Department completed matches with all 1013 Massachusetts banks, the sample data indicates that there may be a conservative potential savings of $110 million.

The $110 million consists of $40 million in on-going savings as a result of caseload reductions and $70 million in recoupment of funds previously paid by the Department to these cases.

It is not known at the present time whether excess asset cases may also be ineligible as a result of other factors such as excess earnings, income, or property holdings, but the volume of fraud already discovered is far too high to be tolerated or ignored.

As of December 3, 1982, 955 Massachusetts public welfare cases have been terminated as a direct result of the bank match program. An additional 1269 cases have received notices of termination and are in the process of review and resolution. 670 cases are pending appeal, and in these cases benefits are continued until the hearing decision.

Preliminary data that has not received a final edit by the Massachusetts Department of Public Welfare indicates that more than 1,600 Massachusetts recipients may hold liquid assets in excess of $5,000 in the bank records matched to date. Among the potential excess asset cases discovered, the following facts have been confirmed: 11 recipients may have liquid assets of more than $100,000 and one individual of $228,972; 45 recipients may have assets between $50,000 and $100,000; 169 recipients may have assets between $25,000 and $50,000; and 1,406 recipients may have liquid assets between $5,000 and $25,000.

Confidentiality of public records has not been an issue in the Massachusetts program. The Massachusetts Department of Public Welfare publishes its intent to verify the assets of welfare applicants at the time of application. An applicant for public aid is informed at the outset on this point and the signed application becomes a form of consent agreement.

In those instances where errors have occurred in matching social security numbers or names, the hearings process provides ample opportunity to verify incorrect or incomplete information and to avoid penalties to those who in fact are eligible recipients.

Incorrect social security numbers has been one of the largest sources of error in the Massachusetts bank match program. Most of the social security number errors have developed during the bank computer runs, since banks are not required to validate the social security numbers contained in their records. To counteract this problem our bank match program is now using a combination of first letters in names plus the social security number to reduce this source of error. In addition, the Office of Inspector General of the United States Department of Health and Human Services is working with the Massachusetts Department of Public Welfare to develop more effective means for validating and verifying social security numbers of welfare recipients for the future.

The bank match program has proved to be a very important tool in reducing waste and fraud. It can be an even more effective tool in future deterrence when asset verification is understood by the public to be an established and ongoing public policy.

However, with public notice and reporting of the bank match program, it is reasonable to expect some movement of assets by welfare recipients. Funds may be withdrawn from deposit accounts and be concealed or invested in out-of-state banks or in other financial yield areas such as mutual funds or money markets which are not yet covered by the state banking laws. We are presently filing legislation to expand the types of financial institutions required to disclose data on welfare recipients to the Department, but in order to assure that only eligible people are receiving welfare benefits, national legislation enabling bank matches across state borders is an essential next step.

I, the Commissioner and the staff of the Massachusetts Department of Public Welfare are prepared to assist your Committee in your work and to answer your questions. Thank you.

ATTACHMENT A

A COMPARISON IN THE PERFORMANCE OF THE MASSACHUSETTS DEPARTMENT OF PUBLIC WELFARE, 1978 to 1982.

		1978	1982
1.	AFDC caseload	121,532	91,000
2.	% change in prior 4 yrs.	+14%	-25%
3.	AFDC Error rate	24.8%	7%
4.	Fraud Referrals	3009	37,019
5.	Guilty findings on fraud	41	800
6.	Child support collection	$25.8 million	$40 million
7.	Number of welfare offices	118	74
8.	Cost of living and benefit increases prior 4 years	12%	15.2%

ATTACHMENT B

COMPUTER MATCHES PERFORMED BY THE MASSACHUSETTS WELFARE DEPARTMENT

Matching Agency	Information Obtained	Statutory Authority[1]	First Time and Frequency of Subsequent Matches
Department of Revenue	Quarterly wage data to verify income reported	Chapter 367, Section 54 Acts of 1978	October, 1980 Weekly for applicants, monthly for recipients
Department of Employment Security	Unemployment compensation data to avoid duplicate payments.	Chapter 367 Section 54 Acts of 1978	February 1982 Weekly for applicants, monthly for recipients
Registry of Motor Vehicles (Excise Tax Division)	Automobile ownership and value as part of assets limit.	Chapter 118[1] Section 3	Expected January, 1983. Will be ongoing part of online system
Commercial Savings Banks and Co-operative Banks in Massachusetts	Asset data	Chapter 18[1] Section 15	June, 1982. One time initiative, will be quarterly.
Veterans Administration	Veterans benefit data to avoid duplicate payments	Chapter 118[1] Section 3	April, 1982. Weekly for applicants, monthly for recipients.
Social Security Administration	Social Security Number Verification	Chapter 118[1] Sections 2B and 3	October, 1978 Monthly for new applications
Group Insurance Commission	Third party insurance liability.	Chapter 18[1] Section 5G	July, 1982. Semi-annual

---

[1] Massachusetts General Laws

ATTACHMENT C

STATUTORY AUTHORITY FOR DEPARTMENT OF REVENUE AND BANK MATCHES

1. CHAPTER 18, SECTION 15 (Effective in 1967, amended in 1973)-- Authorizes requests for bank information.

Disclosure of Information by Banks and Insurance Companies as to Applicant's or Recipient's Deposits; Penalty

"A treasurer of a savings bank, national bank, trust company, co-operative bank, benefit association, insurance company or safe deposit company authorized to do business in the commonwealth who, upon written request, signed by an officer of the department, unreasonably refuses to inform him of the amount deposited in the corporation or association to the credit of a person named in such request as a charge upon the commonwealth, or as an applicant to the commonwealth for public assistance under chapters one hundred and seventeen, one hundred and eighteen, or who willfully renders false information in reply to such request, shall forfeit fifty dollars to the use of the commonwealth. Upon such request, a treasurer as aforesaid shall furnish the records on deposits and withdrawals during the past five years, concerning any applicant for or recipient of public assistance under chapters one hundred and seventeen, one hundred and eighteen, to any officer of the department."

Added by St. 1967, c. 658, §1. Amended by St. 1973, c. 1210, §14.

2. CHAPTER 62C, SECTION 21,(a),(b)(9),(b)(10) (Effective 1980) -- Prohibits disclosure of tax information with listed exceptions.

Fair Information Practices

"(a) The disclosure by the commissioner, or by any deputy, assistant, clerk or assessor, or other employee of the commonwealth or of any city or town therein, to any person but the taxpayer or his representative, of any information contained in or set forth by any return or document filed with the commissioner, other than the name and address of the person filing it, except in proceedings to determine or collect the tax or for the purpose of criminal prosecution under this chapter, chapters sixty A, sixty-two to sixty-five C, inclusive, section ten of chapter one hunderd and twenty-one A and section twenty-one of chapter one hundred and thity-eight is prohibited. (Amended by 1980,c.403, §4, approved, with emergency preamble, July 8, 1980; by §15, effective January 1, 1980.)

(b) Nothing herein shall be construed to prevent

(9) the disclosure to the commissioner of public welfare, upon his written request, of the fact that a specific bank or other entity paying interest income, doing business in the commonwealth has filed for any year a report under section eight with respect to interest paid by it to a designated recipient of public assistance under any program administered by the department of public welfare and of the amount of the interest so reported, together with the identification of the account with respect to which the interest was paid. (Added by 1978, 367, §54, approved July 10, 1978; by §72, effective July 1, 1978; amended by 1981, §801, approved January 13, 1982, effective 90 days thereafter.)

(10) the disclosure to the director of the division of employment security, the commissioner of public welfare or the commissioner of veterans' service of information necessary to ascertain or confirm the existence of fraud, abuse of improper payments to an applicant for or recipient of veterans' benefits. (Added by 1978,c.367, §54, approved July 10, 1978; by §72, effective July 1, 1978.)"

3. CHAPTER 367, SECTION 54A (Effective 1978) -- Authorizes DOR wage matches.

SECTION 54A. "Every employer required to deduct and withhold taxes upon wages, under the provisions of chapter 62B of the General Laws, shall, for each calendar quarter beginning April first, nineteen hundred and seventy-nine submit to the department of corporations and taxation a report of the name, social security account number, and gross wages paid to each employee and any identification number such employer is required to include on a withholding tax return filed pursuant to said chapter and in such form and such manner as may be prescribed by regulations of said department and consistent with federal requirements or limitations.

The department of corporations and taxation shall design, develop, implement, and operate a wage rporting system for the purpose of recieving, maintaining, and processing information required to be submitted by employers pursuant to section two of chapter sixty-two C of the General Laws, for the purposes of verifying eligibility for and entitlement to public assistance benefits, elgibility for and entitlement to unemployment insurance benefits, eligibility for and entitlement to veterans services benefits, underreporting of taxable income, and errors and any fraud or abuse in connection with such benefits paid or income as reported.

Upon the written request of, and at a date specified by, the commissioner of corporations and taxation, the division of employment security shall provide to the department of corporations and taxation lists of all claimants paid unemployment insurance benefits for the purpose of verifying eligibility and detecting and preventing fraud, error and abuse in the unemployment insurance benefits program and other benefits programs administered by said division. Information on such lists shall include the employer's name, the employer's identification number, the claimant's name, the claimant's social security number and other data required for positive identification.

Upon the written request of and at a date specified by the commissioner of corporations and taxation, the department of public welfare shall provide to the department of corporations and taxation lists of applicants and recipients of public assistance for the purpose of verifying eligibility and detecting and preventing fraud, error and abuse in the programs administered by said department. Information in such lists shall include the recipient's name, social security number and other data required to assure positive identification.

Upon the written request of and at a date specified by the commissioner of corporations and taxation, the office of commissioner of veterans' services shall provide to the department of corporations and taxation lists of applicants and recipients of veterans' benefits for the purpose of verifying eligibility and detecting and preventing fraud, error and abuse in the programs administered by said office. Information in such lists shall include the recipient's name, social security number and other data required to assure positive identification.

The department of corporations and taxation shall compare the data provided to it under this section, so as to identify any cases in which individuals who are receiving unemployment compensation, public assistance, or veterans' benefits are also receiving wages. The department of corporations and taxation shall thereupon furnish to the division of employment security , the department of public welfare, or the office of commissioner of veterans' services the cases of any recipients in their respective programs who are identified as receiving wages. The information furnished by the department of corporations and taxation to the receiving agencies shall include the name of the recipient and other data required to assure positive identification, the name and identifying number of the employer, and the amount of income received.

Upon receipt of such information, the division of employment security, the department of public welfare or the office of commissioner of veterans' services shall, with respect to recipients in their respective programs, seek to verify the accuracy of the information presented, in consultation with the recipient whose status is in question.

If after such informal inquiry any of the administering departments concludes that error or fraud has led to incorrect payments to recipients, said department shall take appropriate formal action to correct the situation, provided, however, that no adverse action shall be taken against any recipient except after a hearing affording the recipient full opportunity to contest such action, in accordance with law.

No employee or agent of the commonwealth shall divulge any of the information referred to in this section, except in the manner herein prescribed, to any public or private agency or individual. Unauthorized disclosure of any of this information shall be a violation punishable by a fine of one hundred dollars per offense; provided, that unauthorized release of such information about any individual shall be a separate offense from information released about any other individual. Such unauthorized release of information shall also be cause for administrative discipline of any employee who engages in such unauthorized release.

Any employer who, without reasonable cause, fails to comply with this section and who, after notification by certified mail, return receipt requested, of such failure to comply continues for more than fifteen days, after the mailing of said notice, in noncompliance without reasonable cause shall be liable for a penalty as follows:

for the first failure to comply with said section two: fifty dollars per employee: for the second failure to so comply one hundred dollars per employee; for the third and subsequent failures to so comply: two hundred and fifty dollars per employee. Any employer who willfully and knowingly submits false data or omits accurate data shall be punished by a fine of not more than one thousand dollars or not more than three months in prison."

SECTION 54B: "An advisory committee on the implementation of a wage reporting system is hereby created consisting of two members of the senate, appointed by the president; four members of the house, appointed by the speaker, one of whom shall be a member of the special legislative commission on privacy; the attorney general or his designee, and five persons to be appointed by the governor, one of whom shall represent the Associated Industries of Massachusetts, one of whom shall represent the Massachusetts AFL-CIO, one of whom shall represent the Retailers Association of Massachusetts, one of whom shall represent the Massachusetts Law Reform Institute, and one of whom shall represent the Massachusetts League of Cities and Towns; and three persons to be appointed by the chairman of the state welfare advisory board one of whom shall be a recipient of aid to families with dependent children; one of whom shall be a recipient of general relief; and one of whom shall be a recipient of veterans' benefits.

The governor shall appoint a chairperson from among the membership of the committee members. The committee shall meet from time to time and at a place convenient to its purpose. It may recommend to the departments participating in the wage reporting system and data exchange authorized by section fifty-four A of this act guidelines to assure that accessibility to and exchange of such data shall be restricted to officers and employees of the respective departments participating in the program, that such data and any investigation connected therewith shall remain confidential except for confirmed cases of fraud, that due process shall be observed with respect to the rights of any individual who, as an applicant for or recipient of the public assistance of unemployment insurance benefits or veterans' benefits, is suspected to have provided the respective departments with false or fraudulent information in the removal of identified cases of ineligibility, the recovery of funds disbursed to ineligible recipients, and the referral of identified cases of fraud to the proper authorities for legal action. It shall file a report on the implementation and status of the wage reporting system including any recommendations thereon with the clerks of the house of representatives and the senate no later than July first, nineteen hundred and eighty and every six months thereafter."

SECTION 54C. "Section 17A of chapter 66 of the General Laws, as most recently amended by section 27 of chapter 885 of 1969, is hereby further amended by inserting after the word "assistance", in line 10, the words: including the use of said records by the department of public welfare in concert with related wage reports to ascertain or confirm any fraud, abuse or improper payments to an applicant for or recipient of public assistance."

Senator COHEN. Our next witness is David Linowes, professor of political economy and public policy at the University of Illinois.

I should mention that Professor Linowes is the former chairman of the Privacy Protection Study Commission. Professor Linowes, welcome.

TESTIMONY OF DAVID F. LINOWES, PROFESSOR OF POLITICAL ECONOMY AND PUBLIC POLICY, THE UNIVERSITY OF ILLINOIS

Mr. LINOWES. Thank you, Mr. Chairman. I appreciate the invitation to testify at this hearing. In view of the lateness of the hour, I thought I would identify the highlights of my prepared testimony and add some comments that I think would be appropriate in view of what I heard here this morning.

As you know, it was several years ago that the Privacy Protection Study Commission made over 160 recommendations to the Congress and the President for the protection of privacy. Although many of the recommendations have been implemented by Executive order in Government and by voluntary actions in the private sector, unfortunately, legislation to assure full and uniform compliance has not been enacted. Bills had been introduced in the House and Senate in this Congress and in previous Congresses, but for some reason, they didn't stir up enough general interest to get to the floor with the appropriate sponsorship.

Every time privacy is discussed, everyone professes to strive to assure that a just balance is obtained between the privacy rights of the individual and the management needs of the concerned institutions. Generally, when they talk about management needs, they talk about dollars and cents. But I think we have to recognize that this balance has to take into consideration not just effective use of resources, but the important need to promote credibility and faith in Government, which you cannot have if you're going to have widespread cheating.

As you know, Mr. Chairman, the Privacy Commission was set up by an act of Congress. The Commission was bipartisan and we were given 2 years to complete our mandate. We conducted extensive hearings throughout the country and called several hundred witnesses.

Senator COHEN. Was that in 1977, Mr. Linowes?

Mr. **Linowes**. Yes, we were appointed during the Ford administration and submitted our report during the Carter administration.

In the judgment of the Privacy Commission, the kind of balance that everybody talks about is achieved when we adhere to certain specific operational guidelines. Although our report came in with over 160 recommendations, the essential guidelines are only about 9. Several of them were commented on here today. But I think it's important that we recognize those points. They are not complex.

For example, only information that is relevant to the decision at hand should be collected. And it should be used only for that purpose.

Senator **Cohen**. What about income tax returns?

Mr. **Linowes**. I'd like to comment later on income tax returns. I found the discussion earlier here a little disturbing from personal privacy and administration perspectives.

Senator **Cohen**. I'm sorry. I won't interrupt.

Mr. **Linowes**. To continue, before an organization transfers data to a third person or another agency, it should at least inform the subject personally, not just publication in the Federal Register. I don't believe that's adequate notice. The layman throughout the country doesn't even know such a thing exists. And, if practical, obtain the subjects approval.

Senator **Cohen**. If he could, he couldn't read it in the Federal Register in any event.

Mr. **Linowes**. Yes; the print's too small, and there is so much valued material. [Laughter.]

Also, the individual should be informed which sources will be contacted to get the information, how the data will be used and to whom it will be disclosed. No information should be obtained under false pretenses or through the impersonation of others. Every subject should have the right to see and copy the records about himself from any organization that keeps a file on him, and if he questions the accuracy, have the right to correct that record. If there are points in dispute and there is some credibility to the dispute, the subjects position should also be entered into the record.

There should be no secret files, and records should be destroyed after they have served their purposes.

That's it. Implementing them, however, is another matter. We have been sidetracked constantly over the past several years. I'm convinced that if these points are made an integral part of an agency's policies, we can be assured that the personal privacy dimension of human rights, and it is a dimension of human rights, would be fully protected.

However, subscribing to these essential privacy guidelines does not preclude procedures by the administering agency to assure that all claimants for benefits are eligible. The Commission itself recognized that verification may be necessary, especially when inconsistencies or vagueness of information received from an applicant raised doubt about eligibility. It also believed that State and local agencies, unquestionably, need a degree of flexibility in determining when verification is necessary and from what sources verification may be secured.

Nevertheless, because stigma sometimes attaches to the receipt of public assistance and social services, the Commission believed that there should be some Federal restriction of procedures to be followed, and to some extent we have that by the OMB guidelines. That's to assure that the verification process does not result in more information than necessary about a client being disclosed to third parties and so that there is uniformity throughout the various agencies of Government.

On the specific issue of matching programs by States, I would like to read about three sentences from that report, which is now 5 years old.

I'm quoting:

> The Commission realizes that some States operate automated verification systems in which lists of clients are matched with records maintained by other State agencies, such as State employment agencies. Although the Commission recognizes the utility of such systems in reducing both overpayments and payments to ineligibles, it believes,

And this I want to emphasize—

> that each client should be informed that such methods will be used and offered an opportunity to withdraw his application should he object to this means cf collateral verification. Withdrawal of an application by an individual who is not in fact eligible would, in effect, achieve the desired end—reduction of payments to ineligibles.

But the emphasis there is on visibility, making sure that the subject knows what he's getting into when he applies for assistance.

Sound management practice, on the other hand, requires than an adequate system of internal controls be in place in every operating organization. Internal control is a basic and necessary system for safeguarding assets, checking accuracy, monitoring compliance with rules, procedures, and policies. No management in the private sector or public sector can function effectively without such a system. No audit by professional auditors can be completed without a review and comment upon the adequacy of an organization's internal controls. A property designed matching system is such an internal control procedure.

Matching systems need not result in privacy abuses, so long as adequate protective provisions are built into the system. That's not to say abuses cannot occur, even with fully adequate privacy procedures and policies in place if administrators become overzealous. This overzealousness is the danger. To assure fair administration there must also be adequate enforcement procedures and penalty programs. These we do not now have.

On the other hand, overzealous proponents of exaggerated privacy rights—and we do have such people—can be equally harmful to our democratic institutions. Nothing can destroy a democratic society's institutions faster than the people's loss of faith in their government's credibility and effectiveness.

I believe the "Guidelines for Conducting Computer Matching Programs" issued by OMB on May 19, 1982, makes sound provisions for protecting the privacy rights of the individual, with particular caveats. I particularly note in my written testimony the points that I feel are critical to adequate protection that's built into OMB. I shall not read them here.

I merely want to observe now one important element which indicates that subsequent disclosure of hits—this is in the OMB guidelines—must be done in accordance with the provisions of the Privacy Act.

I should note that in several areas the Privacy Act is found wanting. It is not fully adequate to assure comprehensive personal privacy protections. Because of inadequate enforcement provisions, we have to look to administrators to take the initiative. And I suspect that's one of the reasons that we find this issue sufficiently critical to warrant 2 days of hearings by this important committee—because administrators have been taking the varying initiatives in establishing enforcement mechanisms and penalties.

Mr. Chairman, the Privacy Commission thought that inadequacies of the Privacy Act was so important that, in addition to its over 600-page report, it prepared an appendix called "The Privacy Act of 1974: An Assessment." I'd like to submit this either for the record or for the file of the committee as you see fit.[1] This does point out the weaknesses in the act, although overall it's a good act. After all, it's the first time that legislation, as such, has been enacted dealing with the issue of privacy. It needs substantial review and some limited modification, in particular, concerning the enforcement mechanism and some of the vagueness in the language and some penalty provisions, which we do not have.

Incidentally, on this same subject of act modification, one of our recommendations, and it was an important recommendation was that there should be established an Office of Privacy Protection, not a regulatory agency. It need not be set up by acts of Congress, but by executive order established in the White House for purposes of carrying out the monitoring function.

Of course, if Congress should see fit to establish it, so much the better. But it could be implemented, in any event, without legislation. That would prevent the agencies from "running loose," as you referred to earlier.

Senator COHEN. Do you think that administrations are principally concerned with privacy or with——

Mr. LINOWES. Yes. It would maintain a monitoring function and it would have the ability to identify and point the finger where the enforcement mechanism might be in the hierarchy of the administration.

Right now, there is no centralized authority. OMB is attempting to move in that direction. But OMB has many other, what they consider and I guess what other people consider, more important issues.

Senator COHEN. I can't find anybody in this administration or any other administration that's terribly concerned about these kinds of issues. OMB wants out. Inspectors General certainly aren't going to be the ones to be concerned about treading upon the sensitivities of people's rights of privacy. There isn't really anybody within the Government structure that is too concerned about it.

---

[1] Document retained in subcommittee files.

Mr. **Linowes**. I agree completely with you, and I have been involved, and am involved currently, as adviser to the President's private sector survey on cost control in Government. We deal extensively with the inspectors general. They're overloaded as they are just in trying to monitor over inadequate procedures that limit effectiveness in their areas of responsibility.

I think it's even more critical today than it was 5 years ago that there be such an office. I am not suggesting anything that takes on the semblance of a regulatory agency. We don't need that.

As a matter of fact, one of the reasons we are very often criticized by other countries—Sweden, West Germany, France, many of the other European countries—we do not have such a centralized office. Today, the privacy issue is not just what we're talking about today, but with communications satellites expediting transporter data flow there are no controls, no monitoring, no treaties, no laws to protect sensitive information that's going from country to country. West Germany, France, Sweden, Australia, others, have such laws.

I don't want to digress because the issue that we're facing today is sufficiently important, if for no other reason than because all of the discussion of matching programs requires that it take on the critical urgency for action. But I can understand why it would arise. It is because we are too much dependent upon each administrator to design his own privacy procedures.

Senator **Cohen**. Mr. Linowes, back on February 13, 1978, a Time magazine article reported on the results of Project Match. And in that piece you were quoted as saying that "People shouldn't be treated as so many pieces of raw data being shunted about."

Mr. **Linowes**. Yes. Yes, because we have to weigh both elements—although I don't recall that quote—it may have been part of something else—but I stand by that statement. We're dealing with human beings, and on that point, two of the issues that were raised here earlier would be appropriate to comment on here, that is, the Internal Revenue Service and having the private sector do the matching.

I think private sector matching should be discouraged. If the confidentiality is abused by someone in the private sector and, for that matter, to a limited extent in the public sector, there are no penalties to apply. Our recommendation was that there be general damages, that is, penalties without having to prove any damages, of between $1,000 to $10,000, assessed against the individual, not his office, not his agency, not his bank, but the individual. That will hurt. Such a penalty hurts a person getting say, $20,000 a year, and therefore will be deterred from violating confidential information.

And I feel it's important for another reason that was aired earlier. Our legal establishment in this country works on a contingent fee basis. Impecunious citizens will have access to legal assistance if the lawyer sees the possibility of collecting between $1,000 and $10,000 for his client. He would collect his third or half.

But the critical point is that anybody who is wont to abuse someone's privacy for the fun of it, or for something more serious, would have to think twice if he knows that there's going to be a dollar penalty staring him in the face. And that would again give the individual a sense of power, if you will, to protect himself. They are not just numbers being kicked around as they are presently being handled.

With respect to the Internal Revenue Service, we in this country benefit from something that we take for granted, and I don't think we should. There aren't more than a small handful of countries in the world that have a self-assessment tax structure. We, as individuals, tell the Internal Revenue Service what our income is, what our deductions are, and we pay taxes on it. And, in order to make sure that we do get as honest answers as we can, if you put the wrong figure down on the return or on a form, or forget a figure, you can go to jail. The penalty is very severe.

I don't think the Internal Revenue Service, with the tremendous pressures placed on them, and the need for maintaining the credibility of the taxpayer in his tax-collecting agency, should also be burdened with matching problems, areas that the Congress never thought to be of sufficient importance to also want to assess criminal penalties for violations.

That's not to preclude the use of the Internal Revenue Service for criminal purposes. However, it should be a last resort, in my judgment. I think we can become terribly sidetracked if we begin looking to the Internal Revenue Service, not only to do the matching, but to furnish information to many agencies.

Now to turn to some specific questions that were raised in the letter inviting my participation. There's no question, in my judgment, that matching is most cost effective, especially in view of the speed and efficiency with which this function is carried out today with the computer.

Let me point out that once you design the software, the system for matching, and incur that one-time cost, then the expenses are nominal. The list-matching process is no more often abused, in my judgment, of privacy than what's going on right now by the Internal Revenue Service and is very cost effective. They are now matching the forms 1099—those forms the taxpayer receives when he receives interest income or consultants' fees and honoraria. They match those against the individual's form 1040. That's effective and it's clearly cost effective, as well as helping to build faith and credibility in their operations.

The question which was raised in the letter concerning whether matching is equivalent to a national data bank—clearly not. Especially if the guidelines recommended, such as destruction of records after they've served their purpose, is observed.

With that, Mr. Chairman, I have touched on the highlights of my principal points. I'll be glad to answer any questions you may have.

Senator **Cohen**. Thank you, Professor Linowes. I just have a couple of questions. Do you feel that the guidelines that you recommended in your Commission are being fully implemented now?

Mr. **Linowes**. There's a good attempt at it. There are too many breakdowns at the present time when you say "fully implemented."

Senator **Cohen**. Well, let's talk about notice.

Mr. **Linowes**. No, they are not. The notice, the visibility, is clearly not there. But also, we don't have laws of any consequence that impact the private sector. The Privacy Act of 1974, and this is what the OMB and others are moving to implement, just applies to Government. Now today, because of matching and the interplay between Government and business, unless these protections do bring within their scope the private sector, we really only have half a leg to work with.

And Senator, in direct response to your question, we sorely need those two pieces of legislation that are bottled up somewhere, one dealing with medical records, one dealing with financial records. They are more or less omnibus bills, each dealing with different areas. And it's surprising in view of the enthusiasm with which privacy protection was received by a number of congressional committees. It never got into the chain of procedure for enactment.

Senator **Cohen**. Let me come back to the statement that you made in your opening remarks about only information that is relevant should be collected. That leaves it pretty wide open, in my judgment. For example, I've been reading articles in recent years about new scientific breakthroughs. They can perhaps determine whether someone is genetically or chemically predisposed to violent behavior, antisocial behavior, criminal behavior. So that perhaps, because we do have a real fear of crime in this country, there will be pressure generated to stop criminals before they get at large. Maybe we can start dealing with schoolchildren, for example, at the elementary level. Maybe we can start having doctors and physicians or paramedical people become involved with those children to try and avert future criminal behavior.

Now, in order to get that kind of information, I suppose that school administrators could legitimately claim they are accumulating relevant information such as relevant medical information for the treatment of the child, relevant information pertaining to possible antisocial behavior, and that they are required to start accumulating that kind of information.

So now you have a situation where relevant information is being accumulated on individuals dealing with sexual habits. I've seen some of those questionnaires that go out to schoolchildren. I used to be on a school board and I saw some of the proposals that were submitted for questionnaires to kids about what their private thoughts were, what sort of habits they had, what sort of thoughts generated—particularly the sexual connotation—all sorts of very, I thought, intrusive types of inquiries into the private thoughts of individuals. All of which, if it's allowed to go unchecked, or if it's, in fact, sanctioned by the government, local or Federal, starts building a volume of information on an individual. Then the information is put on records, and is computerized, which then becomes "relevant information", which at some future time we start collecting.

That's sort of what disturbed me when you started talking about not allowing people to be shunted about like raw facts. This gets at that whole issue of intrusiveness. To me, it's much more invidious to have these sorts of transmissions of private, confidential information whipping back and forth between computer banks, unbeknownst to anybody, especially that individual.

And you said that nothing can destroy people's faith in a government more than a lack of credibility. That cuts both ways as well, because you only have, I think, less than 36 democracies left in this world—less than 36. And I could say that nothing can destroy a people's faith in its government more than too much credibility, too much credibility in terms of Warsaw, too much in terms of martial law, too much in terms of what's taking place in the Soviet Union. Or on the fascist governments that we have.

So it cuts—and I'm sure you would agree—both ways. You can have a loss of faith in government if that government stands for the wrong kind of principles, where they are solely interested in collecting information to prevent subversion or any sort of dissent or potential criminal behavior. Suddenly we become wafted into a stratosphere of science, where we don't really concern ourselves with the individual, but we are so preoccupied with what is possible, what is achievable, what is technologically capable, that we forget what separates us as a society. We, like Athens, I think, stand out.

So we've got to be conscious of that. That's what, to me, is so disturbing about all of the discussion, is how quickly we can accumulate information on individuals. It's marvelous. And we can calculate things out. It's remarkable what we can do today.

There isn't very much emphasis being placed upon the things that you talked about. There is virtually no notice taking place. There is virtually no supervision taking place. The OMB guidelines, for whatever their value, are unenforced right now.

So what we're having is a drift into this world of the computer. Now, there's nothing that we can do to hold back the wave of technology. It's here. The microprocessor is going to be part of our lives. I suspect that within 20 years we will see the advent of robotics, with a robot being available to most middle-income people. Much as you have a television set or a car, you will have a robot. And that has all kinds of implications for the future. But what I'm saying is that somehow, throughout this process, we've got to sensitize our Government, ourselves, about what is taking place. And I think there's a very real drift into a state of mind which is solely dedicated to the collection of information.

Mr. LINOWES. Mr. Chairman, may I respectfully urge you to make that kind of a statement on the floor of the Senate as you reintroduce one of these two pieces of major legislation that are now in mothballs because those two pieces of legislation will assure the individual the kind of protections you're talking about. Today we don't have it.

Senator COHEN. Well, I would hope that if I make such a speech, I'll have more of my colleagues here to listen than I do today. [Laughter.]

But thank you very much, Mr. Linowes. I appreciate your testimony.

[The prepared statement of Mr. Linowes follows:]

TESTIMONY of Professor David F. Linowes, Boeschenstein Professor of Political Economy and Public Policy, University of Illinois, before the Subcommittee on Oversight of Government Management of the Senate Committee on Governmental Affairs, Senator William S. Cohen, Chairman, December 16, 1982, Room 3302 Dirksen Senate Office Building.

Thank you for inviting me to testify at this hearing on the matter of computer matching. My interest in this subject arises both from my capacity as former Chairman of the U.S. Privacy Protection Commission, and from my present post as Adviser to the President's Private Sector Survey on Cost Control in the Federal Government. As you know, several years ago the Privacy Commission made over 160 recommendations to the Congress and the President for the protection of the privacy rights of our citizens. Although many of the recommendations have been implemented by executive order in government and by voluntary actions in the private sector, legislation to assure full and uniform compliance has not yet been enacted. The President's Private Sector Survey seeks to recommend ways in which to improve the effectiveness of government operations and is presently nearing the completion of its assignment.

There has been much debate about the issue of computer matching and its impact on the privacy rights of our citizens, particularly on those Americans who find it necessary to seek the assistance of some government agency to obtain a basic minimum living standard. In dealing with the issue of personal privacy in a social-welfare state, I believe it essential for us to strive to assure that a just balance is obtained between the privacy rights of the individual, and the management needs of the concerned institutions.

In the judgment of the Privacy Commission, such a balance is achieved when relationships between the individual and the agency minimizes intrusiveness, maximizes fairness; and provisions are made to permit the individual to legally enforce his expectation of confidentiality, where such expectation is warranted. Implementation of these principles is accomplished by adhering to certain specific operational guidelines:

Only information that is relevant to the decision at hand should be collected, and it should only be used for that purpose. Before an organization transfers this data to a third person or another agency, it should inform the subject, and if practical, obtain his approval.

The individual should be informed which sources will be contacted to get information, how the data will be used, and to whom it will be disclosed. No information should be obtained under false pretenses, or through the impersonation of others.

The subject should have the right to see and copy records about himself from any organization that keeps a file on him.

If he questions its accuracy, he should have the right to correct the record. Where the point is in dispute, a statement explaining his position should be made part of the permanent file. No secret files should exist, and records should be destroyed after they have served their purposes.

Subscribing to these essential privacy guidelines, does not preclude procedures by the administering agency to assure that all claimants for benefits are eligible. The Commission recognized that verification may be necessary, especially when inconsistencies or vagueness in the information received from an applicant raise doubt about eligibility. It also believed that state and local agencies unquestionably need a degree of flexibility in determining when verification is necessary and from what sources verification may be secured. Nevertheless, because stigma sometimes attaches to the receipt of public assistance and social services, the Commission believed that there should be some Federal prescription of procedures to be followed by agencies so as to assure that the verification process does not result in more information than necessary about a client being disclosed to third parties.

On the specific issue of matching programs by states, I would like to quote several sentences from the Privacy Commission Report which was submitted to the Congress and the President on July 12, 1977:

"The Commission. . .realizes that some States operate automated verification systems in which lists of clients are matched with records maintained by other State agencies, such as State employment agencies. Although the Commission recognizes the utility of such systems in reducing both overpayments and payments to ineligibles, it believes that each client should be informed that such methods will be used and offered an opportunity to withdraw his application should he object to this means of collateral verification. Withdrawal of an application by an individual who is not in fact eligible would in effect achieve the desired end -- reduction of payments to ineligibles."

Sound management practice requires that an adequate system of internal controls be in place in every operating organization. Internal control is a basic and necessary system for safeguarding assets, checking accuracy, monitoring compliance with rules, procedures and policies. No management can function effectively without such a system. No audit by professional auditors can be completed without a review of and comment upon the adequacy of an organization's internal controls. A properly designed matching system is such an internal control procedure.

Matching systems need not result in privacy abuses, so long as adequate protective provisions are built into the system. I believe the "Guidelines for Conducting Computer Matching Programs" issued by the Office of Management and Budget on May 19, 1982, makes sound provisions for protecting the privacy rights of the individual. I particularly note its basic points, namely,

1) The subsequent disclosure of "hits" must be done in accordance with the provisions of the Privacy Act.
2) Agencies must consider the legal authority, purpose and description of the match.
3) If subjects have not consented to the match, agencies must consider whether disclosure under the "routine use" exemption would be appropriate. If so, the agency should provide notice in the Federal Register and report to Congress and OMB if this new use is not already contained in the system of records.
4) Only the minimum information necessary to conduct the match should be provided.
5) The source-agency should ensure that all records are accurate, complete and timely.
6) The file should be returned to the source-agency. It will be used and accessed only to match the file previously agreed to. It will not be duplicated. And only information about "hits" will be extracted.
7) As far as possible matches should be conducted by federal agency personnel.

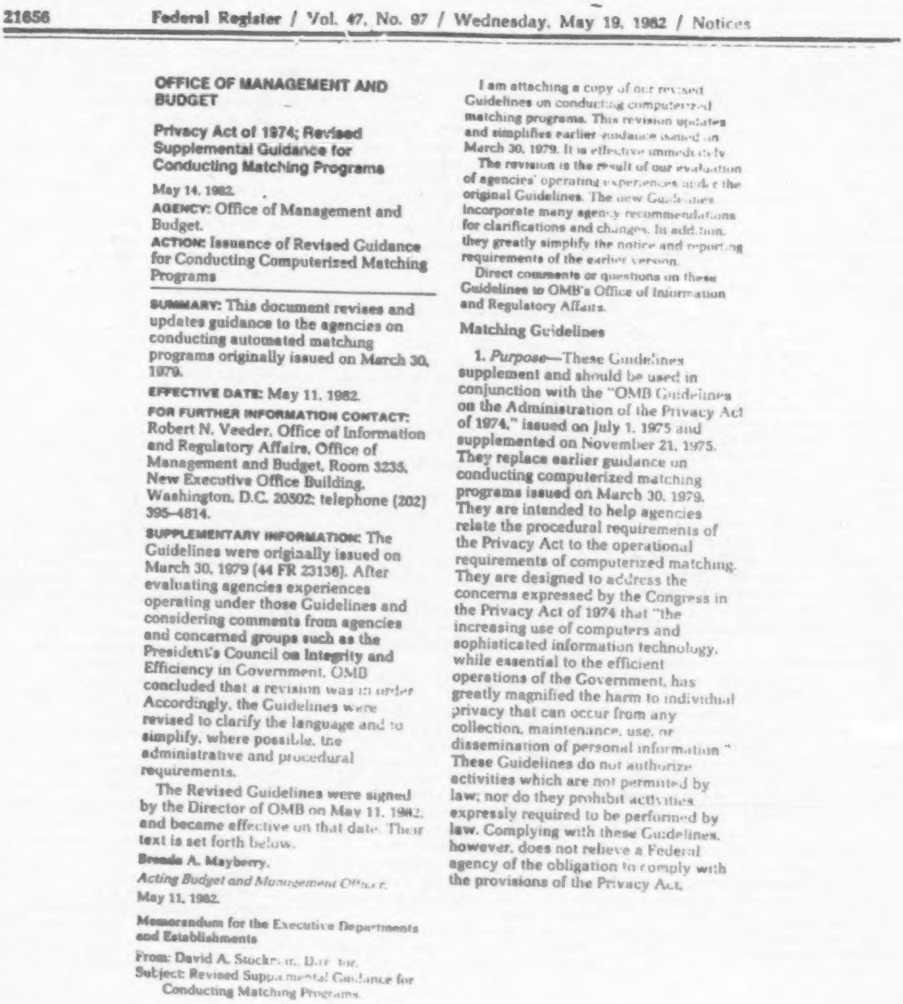
In response to specific questions raised in your letter inviting my participation in this hearing, in my judgment, matching is most cost effective, especially in view of the speed and efficiency with which this function can be carried out today by use of the computer. Further, computer matching cannot be equated to a national data bank, especially if the guideline recommended by the Privacy Commission requiring destruction of the records after they have served their purpose is observed.

I appreciate this opportunity to appear before this Subcommittee on this important issue, and shall be pleased to respond to any questions, or to elaborate on any points I have made in this testimony.

Senator COHEN. The committee will stand adjourned, and we will keep the record open for a period of 30 days.

[Whereupon, at 12:55 p.m., the committee was adjourned to reconvene at the call of the Chair.]

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD



21656 **Federal Register** / Vol. 47, No. 97 / Wednesday, May 19, 1982 / Notices

OFFICE OF MANAGEMENT AND BUDGET

Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs

May 14, 1982.

AGENCY: Office of Management and Budget.

ACTION: Issuance of Revised Guidance for Conducting Computerized Matching Programs

SUMMARY: This document revises and updates guidance to the agencies on conducting automated matching programs originally issued on March 30, 1979.

EFFECTIVE DATE: May 11, 1982.

FOR FURTHER INFORMATION CONTACT: Robert N. Veeder, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 3235, New Executive Office Building, Washington, D.C. 20502; telephone (202) 395–4814.

SUPPLEMENTARY INFORMATION: The Guidelines were originally issued on March 30, 1979 (44 FR 23138). After evaluating agencies experiences operating under those Guidelines and considering comments from agencies and concerned groups such as the President's Council on Integrity and Efficiency in Government, OMB concluded that a revision was in order. Accordingly, the Guidelines were revised to clarify the language and to simplify, where possible, the administrative and procedural requirements.

The Revised Guidelines were signed by the Director of OMB on May 11, 1982, and became effective on that date. Their text is set forth below.

Brenda A. Mayberry,

Acting Budget and Management Officer.

May 11, 1982.

Memorandum for the Executive Departments and Establishments

From: David A. Stockman, Director.

Subject: Revised Supplemental Guidance for Conducting Matching Programs.

I am attaching a copy of our revised Guidelines on conducting computerized matching programs. This revision updates and simplifies earlier guidance issued on March 30, 1979. It is effective immediately.

The revision is the result of our evaluation of agencies' operating experiences under the original Guidelines. The new Guidelines incorporate many agency recommendations for clarifications and changes. In addition, they greatly simplify the notice and reporting requirements of the earlier version.

Direct comments or questions on these Guidelines to OMB's Office of Information and Regulatory Affairs.

Matching Guidelines

1. *Purpose*—These Guidelines supplement and should be used in conjunction with the "OMB Guidelines on the Administration of the Privacy Act of 1974," issued on July 1, 1975 and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concerns expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." These Guidelines do not authorize activities which are not permitted by law; nor do they prohibit activities expressly required to be performed by law. Complying with these Guidelines, however, does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act.

including any provisions not cited in these Guidelines.

2. *Scope*—These guidelines apply to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a), and to all matching programs:

a. Performed by a Federal agency, whether the personal records used in the match are Federal or non-Federal.

b. For which a Federal agency discloses any personal records for use in a matching program performed by any other Federal agency or any non-Federal organization.

3. *Effective Date*—These guidelines are effective on their date of issuance—May 11, 1982.

4. *Definitions*—For the purposes of these Guidelines:

a. All the terms defined in the Privacy Act of 1974 apply.

b. A "personal record" means any information pertaining to an individual that is stored in an automated system of records, e.g., a data base which contains information about individuals that is retrieved by name or some other personal identifier.

c. A "matching program" is a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants.

Matching Programs do not include the following:

(1) Matches which do not compare a substantial number of records, e.g., comparison of the Department of Education's Defaulted Student Loan data base with the Office of Personnel Management's Federal Employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

(2) Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

(3) Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

(4) Matches done to produce aggregate statistical data without any personal identifiers.

(5) Matches done to support any research or statistical project where the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

(6) Matches done by an agency using its own records.

d. A "matching agency" is the Federal agency which actually performs the match.

e. A "source agency" is the Federal agency which discloses records from a system of records to be used in the match. Note that in some circumstances, a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match. The disclosure of records to the matching agency and any subsequent disclosure of "hits" (by either the matching or the source agencies) must be done in accordance with the provisions of paragraph (b) of the Privacy Act.

f. A "hit" is the identification, through a matching program, of a specific individual.

5. *Guidelines for Agencies Participating in Matching Programs*—Agencies should acquire and disclose matching records and conduct matching programs in accordance with the provisions of this section and the Privacy Act.

a. Disclosing Personal Records for Matching Programs

(1) To Another Federal Agency—source agencies are responsible for determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure provisions when they do. Among the factors source agencies should consider are:

(a) Legal authority for the match;

(b) Purpose and description of the match;

(c) Description of the records to be matched;

(d) Whether the record subjects have consented to the match; or whether disclosure of records for the match would be compatible with the purpose for which the records were originally collected, i.e., whether disclosure under a "routine use" would be appropriate; whether the soliciting agency is seeking the records for a legitimate law enforcement activity—whichever is appropriate; or any other provision of the Privacy Act under which disclosure may be made;

(e) Description of additional information which may be subsequently disclosed in relation to "hits";

(f) Subsequent actions expected of the source (e.g., verification of the identity of the "hits" or follow-up with individuals who are "hits").

(g) Safeguards to be afforded the records involved, including disposition.

If the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, it may proceed to make the disclosure to the matching agency. It should ensure that only the minimum information necessary to conduct the match is provided. If disclosure is to be made pursuant to a "routine use" (Section (b)(3) of the Privacy Act), it should ensure that the system of records contains such a use, or it should publish a routine use notice in the Federal Register. The agency should also be sure to maintain an accounting of the disclosures pursuant to section (c) of the Privacy Act.

(2) To a Non-Federal Entity—Prior to disclosing records to a non-Federal entity for a matching program to be carried out by that entity, a source agency should, in addition to all of the considerations in 5a(1) above, also make reasonable efforts, pursuant to section (e)(6) of the Privacy Act, to "assure that such records are accurate, complete, timely, and relevant for agency purposes."

b. Written Agreements—Prior to disclosing to either a Federal or non-Federal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file, e.g.: That the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file(s) previously agreed to; that it will not be used to extract information concerning "non-hit" individuals for any purpose; and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency.

c. Performing Matching Programs—

(1) Matching agencies should maintain reasonable administrative, technical and physical security safeguards on all files involved in the matching program.

(2) Matching agencies should insure that they have appropriate systems of records including those containing "hits," and that such systems and any routine uses have been appropriately noticed in the Federal Register and reported to OMB and the Congress as appropriate.

d. Disposition of Records—

(1) Matching agencies will return or destroy source matching files (by mutual agreement) immediately after the match.

(2) Records relating to hits will be kept only so long as an investigation, either criminal or administrative, is active and will be disposed of in accordance with the requirements of the Privacy Act and the Federal Records Schedule.

e. Publication Requirements—

(1) Agencies, prior to disclosing records outside the agency, will publish appropriate "routine use" notices in the **Federal Register**, if necessary.

(2) If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, the agency involved should publish the appropriate **Federal Register** notice and submit the requisite report to OMB and the Congress pursuant to OMB Circular No. A-108.

f. Reporting Requirements—

(1) As close to the initiation of the matching program as possible, matching agencies shall publish in the **Federal Register** a brief public notice describing the matching program. The notice should include:

(a) The legal authority under which the match is being conducted;

(b) A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose(s) for which the program is being conducted, and the procedures to be used in matching and following up on the "hits";

(c) A complete description of the personal records to be matched, including the source(s), system of records identifying data, date(s) and page number(s) of the most recent **Federal Register** full text publication where appropriate;

(d) The projected start and ending dates of the program;

(e) The security safeguards to be used to protect against unauthorized access or disclosure of the personal records; and

(f) Plans for disposition of the source records and "hits."

Agencies should send a copy of this notice to the Congress and to the Office of Management and Budget at the same time it is sent to the Federal Register.

(2) Agencies should report new or altered systems of records as described in e (2) above as necessary.

(3) Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and the government's effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by section (p) of the Privacy Act or section 3514 of Pub. L. 96-511.

g. Use of Contractors—Matching programs should, as far as practicable, be conducted "in-house" by Federal agencies using agency personnel, rather than by contract. When contractors are used, however,

(1) The matching agency should, consistent with subsection (m) of the Privacy Act, cause the requirements of that Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by FPR Amdt. 155, 41 CFR 1-1.337-5;

(2) The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards and guidelines issued by OMB, GSA, and the Department of Commerce;

(3) The terms of the contrct should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use;

(4) Contractor personnel involved in the matching program should be made explicitly aware of their obligations under the Act, and of these guidelines, agency rules and any special safeguards in relation to each specific match performed.

(5) Any disclosures of records by the agency to the contractor should be made pursuant to a "routine use" (Section (b)(3) of 5 U.S.C. 552a).

6. *Implementation and oversight*— the Office of Management and Budget will oversee the implementation of these Guidelines and shall interpret and advise upon agency proposals and actions within their scope, consistent with section 6 of the Privacy Act.

[FR Doc. 82-13800 Filed 5-18-82; 8:45 am]

BILLING CODE 3110-01-M

OFFICE OF MANAGEMENT AND BUDGET

Privacy Act of 1974; Supplemental Guidance for Matching Programs

AGENCY: Office of Management and Budget.

ACTION: Issuance of guidelines for the performance of computerized matching programs.

SUMMARY: This document is the final version of matching guidelines which were issued for comment in August, 1978. The guidelines apply primarily to matching programs conducted by Federal agencies for the purpose of detecting or curtailing fraud and abuse in Federal assistance programs, or collecting delinquent loan or benefit payments owed to the Federal Government.

EFFECTIVE DATE: March 30, 1979.

FOR FURTHER INFORMATION CONTACT: Leslie Borden Greenspan, Information Systems Policy Division, Office of Management and Budget, Room 9002, New Executive Office Building, Washington, D.C. 20503; telephone (202) 395-3785.

SUPPLEMENTARY INFORMATION: The guidelines were published in proposed form on August 4, 1978 (43 FR 34724). Comments were received from 40 Executive Branch agencies, the General Accounting Office, the Congress, and nine non-Federal organizations. In addition, discussions were held between OMB staff and other concerned agency staff members. The final version reflects to the greatest extent possible the comments received.

The Matching Guidelines were signed by the Director of OMB on March 30, 1979, and issued with President Carter's Message to the Congress on Privacy on April 2, 1979. The text of the guidelines is set forth below.

Velma N. Baldwin,
Assistant to the Director for Administration.

To the heads of executive departments and establishments.

SUBJECT: Guidelines for the Conduct of Matching Programs.

This memorandum forwards guidelines for computer matching of personal records by Federal executive agencies. These guidelines are being issued by OMB to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the need to protect an individual's right to privacy. They are not intended to authorize the performance of matching programs, but rather to provide guidance for matching programs which are othewise justified.

In August 1978 a draft of the guidelines was issued for agency and public comment. Major changes made as a result of the comments received include:

- The guidelines have been extensively restructured and reworded to answer many questions of interpretation which were raised.
- The requirements for agency reporting on matching programs which involve periodic matching of the same kinds of personal records and matching programs for purposes other than curtailing fraud in assistance programs have been simplified to reduce the reporting burden while preserving the opportunity for public comment.
- Criteria for the use of contractors in the conduct or matching programs have been substituted for the stringent limitations on the use of contractors included in the earlier draft.

Any questions regarding these guidelines may be directed to the Information Systems Policy Division (395-3785).

James T. McIntyre, Jr.,
Director.

Matching Guidelines

1. *Purpose*—This document is a supplement to the "OMB Guidelines on the Administration of the Privacy Act of 1974," issued on July 1, 1975 and supplemented on November 21, 1975. It provides guidance to Federal agencies for computerized matching of individuals' records. These guidelines are intended to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the individual's right to personal privacy. These guidelines do not authorize activities which are not permitted by law; nor do they prohibit activities which are not permitted by law; nor do they prohibit activities expressly required to be performed by law. The procedures and limitations set forth in these guidelines apply, even when a statute authorizes or requires a matching program to be carried out, to the extent that these procedures and limitations would not frustrate the

legislative purposes of that statute. Compliance with these guidelines does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these guidelines.

2. *Scope*—These guidelines apply to all agencies subject to the Privacy Act of 1974 and to all matching programs:

a. Performed by a Federal agency, whether the records used in the match are Federal or non-Federal, or

b. For which a Federal agency discloses any records for use in a matching program performed by any other Federal agency or any non-Federal organization.

3. *Effective date*—These guidelines are effective upon the date of their issuance.

4. *Definitions*

a. All definitions in the Privacy Act and OMB Circular No. A–108 apply to these guidelines.

b. A "personal record" means any information pertaining to an individual, stored in a computer system which is retrieved by his or her name or other personal identifier.

c. A "matching program" is a procedure involving the use of a computer to compare a substantial number of records in a Federal system of records with records in one or more other systems of records, or with a set on non-Federal personal records, for the purpose of identifying individuals whose records appear in more than one of the sytems of records or sets of personal records compared. The procedure includes all steps associated with the match, including the acquisition of the records to be matched, the actual use of the computer, and the disposition of information maintained in connection with the match. Checks on specific individuals to verify information provided in an application for benefits, or checks on specific individuals based on information which raises questions concerning the individual's eligibility for benefits which are made reasonably contemporaneously with the application or receipt of the information, are not considered matching programs, regardless of the number of checks made at the same time or that computers are used in making such checks. Matching programs do not include matches performed for the purpose of producing aggregate statistical data which is subsequently used without individual identifiers.

d. An "anti-fraud matching program" is a matching program performed for the purpose of detecting or curtailing fraud or abuse in a Federal assistance program, or for the collection of delinquent loan or benefit payments owed to the Federal Government.

e. A "matching agency" is the agency which performs or seeks to perform, a matching program.

f. A "matching source" is the agency which discloses records to a matching agency for a matching program.

g. A "hit" is the identification, through a matching program, of a specific individual.

h. The "Act" means the Privacy Act of 1974 (Section 3 of Pub. L. 93–579, 5 U.S.C. 552a).

5. *Guidelines for Agencies Conducting Anti-fraud Matching Programs*—Agencies which conducy anti-fraud matching programs using personal records from any other Federal agency, or from a non-Federal organization, should conduct those matching programs in accordance with the provisions of this section.

a. *Development of matching programs*—A matching program should be undertaken only if a demonstrable financial benefit can be realized which significantly outweighs the costs of the match and any potential harm to individuals that could be caused by the matching program, e.g., public disclosure of information about an individual of improper termination of a benefit. The matching agency should consider alternative means of detecting or curtailing fraud and abuse or collecting debts owned to the Federal Government, and should undertake a matching program only if the alternatives are less effective, or more expensive or would present a greater threat to personal privacy. An analysis of the benefits, costs, potential harm, and alternatives considered should be prepared and documented by the agency proposing to conduct the match. This analysis should, as a minimum include:

(1) Estimated losses resulting from fraud, abuse, error, or loan defaults.

(2) Estimates of the number of individuals who are receiving or have received benefits for which they are ineligible, or who have defaulted on loans.

(3) The amount which could potentially be recovered or saved by identification of thos individuals and the termination of improper payments or the collection of delinquent debts.

(4) Potential savings which could be achieved through deterrence of ineligible applicants or through other improvements in the program management (e.g., reduced error rates), based on the matching program.

(5) Estimates of reimbursement costs to be paid to the matching source for the acquisition of records for the matching programs.

(6) Estimates of any cost involved in the actual matching itself, including costs of planning the match, time or effort necessary to make the sets of personal records compatible and the comuter time required for the match.

(7) Estimated costs of follow-up on individual "hits," including verification of individuals' records, locating the individuals, any planned counseling of those individuals, collection efforts, and litigation.

(8) An assessment of the extent to which the conduct of the matching program could discourage individuals from exercising their rights.

(9) An analysis of alternative means for curtailing fraud that were considered and rejected, including a full description of the reasons why they were not considered viable alternatives to conducting a matching program.

b. *Matching reports*—The matching agency should submit a report describing the proposed matching program, consistent with the provisions of this section, to the Director of OMB, the Speaker of the House of Representatives, and the President of the Senate 60 days before a matching program is initiated. If the matching program will involve or result in the establishment or significant alteration of a system of records subject to the Privacy Act, the matching report should be submitted as a part of a Report on New or Altered Systems as required by OMB Circular No. A–108, as amended. If the records to be disclosed by the matching source are to be "maintained" (as defined in subsection (a)(3) of the Privacy Act), by the matching agency, the matching agency must publish a system notice for those records. In addition, the records on "hits" may constitute a system for which a system notice must be published. The advance notice period may be waived by OMB in the same manner as provided in OMB Circular No. A–108. In those cases where the agency determines that compliance with these guidelines would frustrate the purpose of a statute which requires matching of records, the matching report shall set forth the basis for the agency's determination and clearly identify those portions of the guidelines which would frustrate the statutory requirement.

(1) One time matching programs—For one time matching programs the report should include a copy of the agency's analysis of benefits, costs and potential harm prepared in accordance with 5. (a) above, and a description of the matching program, including—

(a) The starting and estimated completion dates of the program.

(b) A description of the personal records to be matched.

(c) The system name(s), date(s) and page(s) of the most recent publication in the **Federal Register** of system notices for systems used to perform the matching program. This includes systems of records maintained by both the matching agency and the matching source.

(d) The source(s) from which records will be obtained and a copy of the routine use or description of any other authority by which records will be disclosed.

(e) The procedures to be followed, both in the actual matching, and in following up on "hits."

(f) A discussion of how individuals' privacy and other rights will be protected, for example, limitations on the amount of information maintained, or on improper access to records.

(g) The safeguards to be applied in the design and operation of the matching program to protect against unauthorized access or disclosure of personal records, consistent with the requirements of OMB circular No. A–71, Transmittal Memorandum No. 1 dated July 27, 1978.

(h) The kinds of records which will be disclosed as a result of the match and those to whom records will be disclosed, including the basis for any routine uses.

(i) The plans for disposal of records developed in connection with the conduct of the matching programs, including the records on "hits" and any additional information maintained on the "hits."

(j) An identification of all Federal and non-federal organizations (including contractors) involved in performing the match and the roles to be performed by each organization.

(2) Continuing matching programs—Continuing matching programs (e.g., a monthly or semi-annual match of recipients of a benefit against the Federal payroll, or a series of matches of the Federal payroll against similar personal records from several States) should be reported as follows:

(a) Initial report—In addition to the information required in one-time matching reports specified in 5(b)(1) above, the initial report for a continuing matching program shall include a discussion of the justification for performing periodic matches of the same kinds of records, an indication of how often the matches will be performed, and a discussion of the relationship, if any, between the periodic matches (e.g., whether new files of the "hits" are created and matched against earlier "hits," and the disposition of those records).

(b) Renewal report—The matching agency should submit a renewal report to OMB and the Congress annually for as long as the program continues. The renewal report should provide justification for continuing the matching program and an evaluation of the previous year's results. The renewal report should describe the results of the previous year's activity, including aggregate data on the number of "hits" in each match, the disposition of those cases, the cost to date of the program, the estimated amounts of money saved or recovered through the program, and the disposition of personal records, consistent with paragraph d. (3) below; and any changes to be made in the matching program as a result of the previous year's experience. The matching agency may submit an annual consolidated renewal report on all continuing matching programs subject to this section, provided that all matching programs initiated within the preceding 12 months are included.

(c) Change report—The matching agency should submit a revised matching report to OMB and the Congress 30 days before obtaining records from a new matching source, changing the kinds of records used, or the kinds of disclosures made. This report should include a description of the changes made and a copy of the initial report. If a system of records is established or significantly altered by the change, a Report on New or Altered Systems must be submitted 60 days before the system is established or altered.

c. *Operating requirements*—Anti-fraud matching programs should be conducted in accordance with the following guidelines:

(1) Use of contractors—Matching programs should, to the maximum extent practicable, be conducted "in-house" by Federal agencies, using agency personnel, rather than by contract. When contractors are used:

(a) The matching agency should, consistent with subsection (m) of the Act, cause the requirements of the Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by FPR Amdt. 155, 41 CFR 1–1.337–5.

(b) The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards and guidelines issued by OMB, GSA, and the Department of Commerce.

(c) The terms of the contract should preclude the contractor from using, copying, or retaining records associated with the matching program for the contractor's own use.

(d) The contractor personnel involved in the matching program should be explicitly made aware of their obligations under the Act, these guidelines, agency rules and any special safeguards in relation to each specific match performed.

(e) Disclosures of records by the agency to the contractor should be made pursuant to a routine use.

(2) Acquisition of records—The matching agency should not acquire records for use in a matching program other than in accordance with these guidelines. The matching agency should provide the matching source with any information necessary for the source to make an informed decision on the appropriateness of disclosing information for the proposed match. (See section 6.) As a minimum, the matching agency should provide the matching source with copies of the analysis of benefits, costs, potential harm and alternatives developed under 5.a above, and a written statement outlining the plans for the match, including:

(a) A description of the personal records to be disclosed by the source.

(b) A description of the personal records against which they will be matched.

(c) The dates when the records will be disclosed by the source and the dates when they will be returned to the source or destroyed.

(d) A description of additional information which may subsequently be requested of the source in relation to "hits," (e.g., detailed payroll information on "hits").

(e) Subsequent actions expected of the source (e.g., verification of the identity of the "hits" or follow-up with matching source employees who are "hits").

(f) The methodology to be used for allocation of any costs of conducting the matching program between the matching agency and the matching source, and any related understanding in regard to financing or transfer of resources in connection with the match.

(g) Any limitations on redisclosure of information provided to the matching agency by the matching source or to disclosure of any information provided to the matching source as a result of the match.

(3) Disclosure of matching program records—Disclosures of personal records which result from the matching program should be made only under the

conditions specified in subsection (b) of the Privacy Act, the 1975 OMB Guidelines, and these guidelines, unless another statute specifically requires a disclosure which is not provided for in the Privacy Act. While subsection (b) of the Privacy Act establishes various conditions for disclosing records without the advance written consent of the subject, disclosures made in connection with a matching program should be made, to the extent possible, pursuant to the routine use provisions, as outlined in (a), below. Dislcosures made pursuant to other provisions of subsection (b) of the Privacy Act, or pursuant to another statute, should be made as outlined (b), below. Disclosures of personal records maintained in connection with the matching program should disclose no more information than necessary, and should disclose information to as few recipients as possible. Disclosures should be made only as necessary to conduct or achieve the purpose of the matching program, and should be made only with the prior written approval of the matching agency official who is responsible for the system of records.

(a) Routine uses—The matching agency shall, consistent with subsection (e)(11) of the Act, publish in the **Federal Register** a notice describing any routine uses of personal records maintained in connection with the matching program. The description of the routine use should clearly indicate that it is associated with a matching program. In addition, the notice should explain the justification for the routine use, including how the disclosure is compatible with the purpose for which the information was collected, and indicate why the records cannot be disclosed without individual identifiers. After publishing the routine use notice in the **Federal Register** and allowing 30 days for public comment, the matching agency should consider any comments which have been received, and revise the routine use as appropriate. After the expiration of the 30 day comment period, the routine use notice should be republished if it has been revised based on comments received. If the routine use is not revised because no comments were received or the comments did not warrant a revision, the matching agency should publish a short notice indicating that the routine use is adopted as originally published, and, if comments were received, indicating the basis for their rejection. The routine use may become effective (i.e., disclosures may be made) immediately following the initial 30-day comment period.

(b) Other disclosure—The matching agency should determine and give notice of any kinds of disclosures which it will make in relation to the matching program, other than those made pursuant to a routine use. The notice should be published in the **Federal Register**, outlining the conditions under which the disclosures will be made and the justification and legal authority for making those disclosures. This notice should be published prior to the conduct of the match and concurrent with the publication of any new or revised system notices or routine uses when applicable.

(4) Limitations on redisclosure—Whenever the matching agency discloses any records which result from a match program, including but not limited to those pertaining to "hits" which result from a matching program, the agency should as an express condition of the disclosure, provide a statement to the recipient which sets forth:

(a) The use to which the records will be put by the recipient.

(b) A stipulation that the recipient will disclose them further only where required by law or where (e.g., in the case of a law enforcement or administrative agency) such disclosure is compatible with the purpose for which the records were originally disclosed to the matching agency by the matching source.

(c) The date by which the records transferred will be destroyed or returned to the matching agency, or, if it is necessary that the records be retained by the recipient, a written explanation of why they are being retained.

d. *Termination of matching programs and disposal of records*

(1) Records obtained from the matching source—Personal records obtained from the matching source should be destroyed or returned to the source within six months after the match takes place. However, if the same system of records is used in a continuing matching program, it need not be returned or destroyed until 6 months after the final match takes place.

(2) Records of "hits"—Unless otherwise required by Federal records schedules, any records related to the "hits," including computer printouts listing the "hits" and any additional personal information compiled on the "hits," should be destroyed within six months after the match unless they are necessary for the completion of pending law enforcement or administrative activities consistent with the purposes of the matching program and authorized by law. Any extension of the six month period should be published, and with appropriate explanation, in the **Federal Register**.

(3) Notification to OMB—The matching agency should notify OMB in writing of the completion of a one-time matching program and the destruction or return of the personal records to the matching source. Disposition of records associated with continuing matching programs should be reported to OMB as a part of the renewal report required by paragraph b(2)(b), above.

5. *Guidelines for Matching Source Agencies Participating in Anti-fraud Matching Programs*

a. *Applicability.* Disclosures of personal records to any other Federal agency or non-Federal organization for the purpose of anti-fraud matching programs shall be made in accordance with the provisions of subsection (b) of the Privacy Act, related portions of the 1975 OMB Guidelines, and provisions of this section.

b. *1975 OMB Guidelines.* While the 1975 guidelines apply in their entirety, selected portions are restated below to stress matching source responsibilities regarding disclosure of personal records.

(1) The 1975 Guidelines pertaining to disclosures of records without the advance written consent of the subject provide that:

"Disclosure, however, is permissive not mandatory. An agency is authorized to disclose a record (without the advance written consent of the individual to whom the information pertainw] *when it deems that disclosure to be appropriate and consistent with the letter and intent of the Act and these guidelines.*

"Nothing in the Privacy Act should be interpreted to authorize or compel disclosures of records, not otherwise permitted or required, to anyone other than the individual to whom a record pertains pursuant to a request by the individual for access to it.

"Agencies shall not automatically disclose a record to someone other than the individual to whom it pertains simply because such a disclosure is permitted by this subsection. Agencies shall continue to abide by other constraints on their authority to disclose information to a third party including, where appropriate, the likely effect upon the individual of making that disclosure. Except as prescribed in subsection (d)(1), (individual access to records) the Act does not *require* disclosure of a record to anyone other the individual to whom the record pertains." (emphasis added) (40 FR 28949, at 28953, July 9, 1975).

(2) The 1975 Guidelines pertaining to intra-agency transfers of information provide that—

"This provision (subsection (b)(1)) is based on a "need to know" concept * * * It is recognized that agency personnel require access to records to discharge their duties. In discussing the conditions of disclosure provision generally, the House Committee said that 'it is not the Committee's intent to impede the orderly conduct of government or delay services performed in the interests of the individual. Under the conditional disclosure provisions of the bill 'routine' transfers will be permitted without the necessity of prior written consent. A 'nonroutine' transfer is generally one in which the personal information on an individual is used for a purpose other then originally intended.' (House Report 93–1416, p. 12).

"This discussion suggests that some constraints on the transfer of records within the agency were intended, irrespective of the definition of agency. Minimally, the recipient officer or employee must have an official "need to know." The language would also seem to imply that the use should be generally related to the purpose for which the record is maintained." (40 FR 28949 at 28954).

c. *Matching source decision on participating in an antifraud matching program.* When a Federal agency is asked to disclose personal records to another Federal agency or any non-Federal organization for the purpose of conducting an antifraud matching program, it sould carefully review the information provided by the matching agency pursuant to paragraph 5c(2) and determine the appropriateness of disclosing the requested information for the proposed matching program. The review should include consideration of the authority for and purpose of the matching program, the appropriateness of disclosing the records for that purpose the procedures to be followed, and any disclosures of the results of the matching program by the matching agency. The matching source may seek any additional information necessary to make an appropriate disclosure decision. The matching source should indicate in writing is concurrence with the matching agency's statement describing the matching program, as provided for in section 5c(2) of these guidelines.

d. *Disclosure of records.* While subsection (b) of the Privacy Act establishes various conditions for disclosing personal records without the advance written consent of the subject, disclosures of personal records by a matching source made for the purpose of conducting a matching program should only be made pursuant to the routine use provisions, as outlined below, unless otherwise required by statute. In those cases where the agency determines that establishment of a routine use would be contrary to other statutory requirements, it should publish a notice in the **Federal Register** outlining the statutory basis for the disclosure in lieu of publishing a routine use notice. In all other cases, the agency should publish a notice in the **Federal Register** describing routine uses associated with proposed matching program(s). The routine use notice should—

(1) Be as specific and limited as possible.

(2) Expressly state that the routine use is intended to permit the disclosure of records for a matching program.

(3) Identify the matching program.

(4) Set forth any conditions which the matching source has established for the use of the records by the matching agency in addition to those set forth in these guidelines.

(5) Include an explanation of how the disclosure is compatible with the purpose for which the records were collected or a citation of the statute requiring disclosure.

7. *Guidelines for Conducting Other Matching Programs*

a. *Applicability*—The reporting requirements of this section apply to—

(1) All matching programs conducted by a Federal agency for other than anti-fraud purposes, using personal records from any other Federal agency or from a non-Federal organization; and

(2) All matching programs conducted by a Federal agency which use only personal records maintained by that agency, except—

(a) Matches conducted for internal administrative purposes using personal records pertaining to agency employees and military personnel and their dependents and not conducted for the primary purpose of detecting fraud and abuse; or

(b) Matches conducted for research or statistical purposes which do not affect individual entitlements.

(b) *Reporting requirements*—All matching programs subject to the provisions of this section should be reported to the Director of OMB, the Speaker of the House of Representatives and the President of the Senate as follows:

(1) Within 90 days of the effective date of these guidelines, the matching agency should submit a report to OMB and the Congress describing any matching programs in progress on the effective date, and plans, if any, for continuing these programs. Any current plans for initiating new matching programs within a year after the effective date of these guidelines should also be included in this report. The purpose of this report is to inform OMB and the Congress of the magnitude and nature of matching programs being conducted or planned and determine the need for developing additional guidelines for matching programs. These matching programs need not be suspended before being reported. The report shall include, for each matching program—

(a) The name and purpose of the program.

(b) The authority under which it is to be conducted.

(c) The approximate dates on which the program will begin and end.

(d) A description of the personal records to be matched; and, if one or both are systems of records subject to the Act, the system name(s) and the date and page of most recent publication in the **Federal Register.**

(e) The procedures to be followed, including disposition of the records.

(2) A matching report shall be submitted to OMB and the Congress by the agency as soon as practicable before a match is performed for any one-time matching program or before the initial match of a continuing matching program which is not included in the report on matching programs submitted pursuant to paragraph b(1) above. The matching report should contain the information outlined in paragraph (b)(1) above.

(3) For any matching program which necessitates the establishment or significant alteration of a system of records subject to the Privacy Act, a Report on New or Altered Systems must be submitted 60 days before the initial match is performed, and any necessary system notices and routine uses must be published in the **Federal Register.**

(4) A Federal agency which discloses records to a non-Federal organization should report the disclosure to OMB. The report should describe the nature of the disclosure and the agency's basis for making the disclosure.

8. *Implementation and oversite*—The Office of Management and Budget will oversee the implementation of and shall review, interpret and advise upon agency proposals and actions under these guidelines, consistent with Section 6 of the Privacy Act.

[FR Doc. 79-12057 Filed 4-17-79; 8:45 am]

BILLING CODE 3115-01-M

COMPARISON OF OFFICE OF MANAGEMENT AND BUDGET GUIDELINES FOR CONDUCTING COMPUTER MATCHING PROGRAMS ISSUED MAY 19, 1982, WITH EARLIER GUIDELINES ISSUED APRIL 18, 1979

This report provides an analysis of the Guidelines issued for federal agencies by the Office of Management and Budget (OMB) on May 19, 1982 regarding computer matching programs. (47 Fed. Reg. 21656). These Guidelines revise and update former guidelines issued by OMB on March 30, 1979. (44 Fed. Reg. 23138). The purpose of the Guidelines is to help agencies relate the procedural requirements of the Privacy Act of 1974, Publ. L. No. 93-579, to the use of computerized matching programs. The Guidelines do not relieve a federal agency of its obligation to comply with provisions of the Privacy Act, but rather are designed to aid agencies in complying with Privacy Act provisions. (Section 1 of 1982 Guidelines).

A "matching program" is defined in Section 4c of the 1982 Guidelines as follows:

> c. A "matching program" is a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants.
>
> Matching Programs do not include the following:
>
> (1) Matches which do not compare a substantial number of records, e.g., comparison of the Department of Education's Defaulted Student Loan data base with the Office of Personnel Management's Federal Employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

(2) Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

(3) Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

(4) Matches done to produce aggregate statistical data without any personal identifiers.

(5) Matches done to support any research or statistical project where the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

(6) Matches done by an agency using its own records.

A number of changes have been made in the 1982 revisions to the Guidelines as issued in 1979. The principal changes include the elimination of the 1979 Guideline requirement of a cost-benefit analysis before performing a matching program, fewer notice and reporting requirements on the part of the agency conducting the matching program, and elimination of the provisions covering intra-agency matching programs as contained in the 1979 Guidelines.

Section 5a of the 1979 Guidelines provided that an agency should undertake a matching program only if "a demonstrable financial benefit" could be realized which would significantly outweigh the costs of the match and any potential harm to individuals that would be caused by the matching program. This cost-benefit analysis requirement was completely eliminated in the revised 1982 Guidelines.

Reporting requirements under the 1982 Guidelines have been significantly streamlined as compared to the reporting requirements of the 1979 Guidelines. For example, under the 1979 Guidelines, a matching agency was required to submit a report describing the proposed matching program to the Director of OMB and Congress sixty days before initiation of a matching program. Also required was a "Report on New or Altered Systems" pursuant to OMB Circular No. A-108 where appropriate. In addition, reports were required for continuing matching programs, and "change reports" were required to be submitted by the matching agency to OMB and the Congress where certain revisions to the matching program were proposed. Under the revised 1982 Guidelines reporting requirements have been substantially reduced. The new provisions require that, as close to the initiation of matching programs as possible, the matching agency publish a brief notice in the Federal Register describing the matching program. A copy of this notice should be sent to the Congress and OMB at the same time. New or altered systems of records continue to be subject to the requirements of OMB Circular No. A-108. However, no other notice or reporting requirements are imposed, although Section 5f(3) of the 1982 Guidelines instructs agencies to be prepared to report on matching programs pursuant to Privacy Act or Paperwork Reduction Act provisions.

The disclosure provisions have also been somewhat revised in the 1982 Guidelines. Where an agency determines that disclosure of records would not violate its responsibilities under the Privacy Act, it may make a disclosure of personal records to another federal agency in order to conduct a matching program. (Section 5a of 1982 Guidelines). While publication of "routine uses" in the Federal Register is required where appropriate under the Privacy Act, the thirty day public comment periods of the 1979 Guidelines have been eliminated. If disclosure of personal records is to be made to a non-federal entity the same requirements pertaining to disclosure to a federal agency apply, with the additional requirement that reasonable efforts be made "to assure that such records are accurate, complete, timely, and relevant for agency purposes", as required by the Privacy Act. (Section 5a(2) of the 1982 Guidelines). In the case of disclosures to both federal and non-federal entities the disclosing agency should also require written assurances that the personal records will be used for only authorized purposes. Contrary to the 1979 Guidelines, the 1982 Guidelines do not require that matching agencies provide notice in the Federal Register of disclosures other than routine uses which it will make in relation to a matching program.

The requirements under the 1982 Guidelines regarding the use of contractors remain substantially similar to those in the 1979 Guidelines.

Also eliminated in the 1982 revisions are the requirements of Section 7 of the 1979 Guidelines relating to matching programs conducted by a federal agency which uses personal records maintained by that agency, i.e., intra-agency matches. Such intra-agency matches are specifically exempted from the 1982 Guidelines under Section 1c which states that "Matching Programs do not include ... (6) matches done by an agency using its own records."

In summary, the 1982 Guidelines for conducting computer matching programs significantly simplify the administrative requirements of the earlier, 1979 Guidelines. In particular, the notice and reporting requirements have been streamlined, and other requirements not directly imposed by the Privacy Act of 1974, such as the cost-benefit analysis requirement as contained in the 1979 Guidelines, have been eliminated.

Kathleen S. Swendiman

Kathleen S. Swendiman
Legislative Attorney
October 22, 1982

U. S. Department of Labor

Inspector General
Washington D.C. 2021

NOV 18 1982

MEMORANDUM FOR: Participants in the Long Term Computer Matching Project

SUBJECT: Reference Paper on Computer Matching

The attached reference paper was developed in response to questions and requests for interpretations by agencies regarding the revised Office of Management and Budget Guidelines on Computer Matching which went into effect on May 11, 1982. The purpose of the paper is to provide advice and suggestions on the intent and contents of the Guidelines in order to assist agencies engaging in matching activities to comply with them. We are distributing the paper as a service to the computer matching network.

RICHARD P. KUSSEROW
Inspector General
Department of Health and
Human Services
Project Co-Chairman

ROBERT E. MAGEE
Acting Inspector General
Department of Labor
Project Co-Chairman

Reference Paper on Computer Matching

Introduction

This reference paper is an outgrowth of the July 1, 1982 interagency briefing and discussion on the Office of Management and Budget Guidelines on Computer Matching. It provides further details and recommendations to assist agencies in complying with the Guidelines provisions. The Guidelines are designed to give direction to agencies in the use of advanced technology in managing government programs while retaining appropriate privacy safeguards.

Definitions

The definitions contained in the revised Guidelines for the most part are unchanged from the previous Guidelines or are self-explanatory. The following comments, however, may prove helpful in supplying further information and interpretation.

Section 4.c.(1) in referring to "a substantial number of records" is flexible in order to confer a reasonable degree of latitude. "Substantial" should usually be interpreted to be a small percentage or quantity of the records which are included in the matching program. Decision on what constitutes a substantial number is a matter for agency management to address.

Section 4.c. enumerates efforts not included in the term "matching programs." While not specifically mentioned, matches which do not use computers, i.e., manual matches, are also not subject to the Guidelines. In addition, matching involving a file of decedent records with a file on living persons is not covered by the Guidelines since the coverage of the Privacy Act is limited to living persons--at least two files of living persons must be involved for these Guidelines to apply. It should be noted, however, that even though the Guidelines do not apply in the particular instances specified in this section, the Privacy Act of 1974 still has overall applicability to the use or disclosure of personal records on living persons.

Planning

Section 5.a. of the revised Guidelines specifies the factors which should be considered by a source agency before it discloses records for matching programs. Section 5.b. provides for written agreement by the matching agency on the use, safeguarding and disposition of personal records supplied by a source agency. Section 5.f.(3). covers annual reporting by agencies on matching activities under two broad headings--protection of individual privacy and effective use of information technology. Detailed advance planning based on careful analysis, particularly on the part of the matching agency, is essential in order to enable agencies to satisfy these provisions of the Guidelines.

As a first step, an agency considering initiation of a matching effort should conduct a thorough and indepth review and analysis of the problems which gave rise to the proposal to undertake a match. This is necessary in order to describe the scope and purpose of the matching, identify the agencies and records which would be involved and determine the information and the follow up actions that would be needed. A key aspect of such an analysis, as discussed below, is an assessment of the projected estimated costs and benefits of a match, so that a decision can be reached as to whether a match effort would be worthwhile. In the analytical process, examination of such possible indicators as past audits, previous matching activities, operational and field reports, public complaints and press criticisms might all prove relevant and helpful for laying out the parameters and implications of the proposed matching program.

Once the analytical review has been completed, detailed planning and design of the match can be undertaken. Procedural details such as the steps and timing involved in the match activities should be developed. Particular attention should be given to the volume of records affected, the data elements to be captured and, most important of all, the staff resources and computer time that will have to be invested. At this stage, a matching agency should be in a position to provide a source agency with specific information about the match, as called for in Section 5.a., a commitment regarding the use, safeguarding and disposition of records, and public notice regarding the specifics of a matching program.

Cost/Benefit Analysis

Agencies must take care that every effort is made that only cost/effective, beneficial matching programs are undertaken. This is a basic agency management responsibility and managers must be held personally accountable that their management initiatives are well formulated and cost effective, with benefits that clearly outweigh possible liabilities.

Cost/benefit analysis should be conducted on both a prospective and retrospective basis. Before a match is undertaken, the best possible projections should be made of the estimated costs involved and estimates of the expected pay back that will stem from the effort. Previous matches and audits should be analyzed and required staff and computer time investments from planning to follow up should be estimated. Depending on how good a projection is possible, a pilot match based on a scientific sample may be a means to get a better idea of what a full-fledged matching effort might produce. Under the new guidelines, pilot efforts are possible but it should be noted that pilot matches are subject to Privacy Act safeguards and where appropriate the requirements for new/altered system reports to OMB and Congress. Particularly if a matching approach is new and no previous parallel experience and results are available for consideration, a well chosen sample should provide indications of how many hits might be anticipated, how much investigation and follow up might prove necessary, how much money in overpayments might be involved and even how much might be saved or recovered. On such a basis, a well founded decision as to whether a match will prove worthwhile should be possible.

Retrospectively, systematic cost/benefit analysis should be conducted, including considerations that could not be taken into account, fully, in a prospective effort. All resources which were brought to bear for the matching effort and follow up, including staff time for planning, analysis, developing and running programs and investigation and costs such as computer time must be tabulated. Results such as recoupments and recoveries, cost avoidance, prosecutions and convictions, and development of preventive system changes and improvements such as computer screens, additional eligibility verification methods and new or amended statutes, regulations, policies and program procedures should be taken into account and assessed. Wherever possible, quantification is desirable, but the emphasis should always be on realism. Soft, indefensible claims for dollar savings should be carefully avoided. It should also be kept in mind, however, that it may not prove possible to quantify some extremely important potential costs and benefits. These include the possible cost of adverse implications or harm to the rights and privacy of individuals and the possible benefit of deterrence, virtually impossible to measure but a very real product of computer matching efforts. Rigorous analysis of the cost and benefit factors should form the basis for solid findings on the effectiveness and desirability of the match.

Publication of Notices

Notices of new systems and routine use publications in general remain the same. It should be noted, however, that published routine uses should be general enough with respect to the jurisdictions to which disclosure is made in order to avoid needless burden and delays, i.e., if records will be made available to all the States or to hundreds of cities for the same program management purpose, a single routine use publication, rather than 50 or hundreds of separate routine use publications would suffice. At the same time, a routine use publication should, wherever feasible, include the specific statement that the information disclosed will be used for computer matching.

A new element in the revised Guidelines is inclusion of a provision (Section 5.f.(i)) for public notice in the Federal Register. There are two reasons for informing the public that computer matching is occurring. First of all, the provision supports the principle of openness in Government and underlines the fact that the Inspectors General and their counterparts pursue their activities openly wherever possible. Secondly, there is hope that public notice of efforts to prevent and detect fraud and abuse may have a deterrent effect.

The revised Guidelines provide that the public notice should be published "as close to the initiation of the matching program as possible." This wording was adopted to provide for flexibility. Ordinarily, however, in the general course of events, agencies should publish notices before the match is attempted and there should be a reasonable time for comments.

Recommendations on the formulation of the public notice and its preamble for the Federal Register are included in Attachment 1.

Record Keeping

Agencies must maintain complete, detailed records on their matching activities as they are proceeding. If the Guidelines are followed carefully, this should not pose problems. One of the primary objectives of the Guidelines revision, laid down from the beginning of the process, was to ensure the existence of complete documentation on matching programs agencies conduct. The reason was to provide a clear, definitive audit trail on matching activity, should there ever be public or Congressional inquiries or should reporting on matching activities be requested. Thus, the Guidelines include a written statement on proposed matches from the matching to the source agency, regarding such matters as the purpose of the projected match, the records involved, the data elements needed and the necessary follow up activity. A written agreement by the matching agency covering the use, safeguarding and disposition of personal records was also included. In addition, public notice in the Federal Register and written notice to the Congress and OMB announcing that a match will be or is being undertaken with specifics concerning the matching program are also specified. Systematic retention of these documents, along with the results of internal analysis, planning and cost/benefit studies, should enable agencies to describe their matching activities with little difficulty and should provide sufficient data to satisfy inquiries of any sort.

ATTACHMENT 1

Guidance for Computer Matching Reports Published in the Federal Register

Preamble

AGENCY: This section should indicate the agency performing the match.

ACTION: This section should state the specific action proposed, i.e., notice of a matching program, including the name of the match.

SUMMARY: This section should include a concise statement which, at a minimum, should indicate the following:

- the identification of the matching agency and the major agency component, if any, performing the match;
- the identification of the source(s);
- a brief statement describing the match.

DATES: This section should include either the specific starting date if known or an approximate projected date--this may be general in the sense of naming a month rather than a specific day within the month.

ADDRESS: This section should include the complete address where the public may send any comments on the match.

FOR FURTHER INFORMATION CONTACT: This section should include the name, title, business address and business phone number, which the public should use when requesting additional information about the match.

SUPPLEMENTARY INFORMATION: This section should include the following:

- any relevant and appropriate background information

- a citation to the new Office of Management and Budget computer matching guidelines. This may be written as follows: "Set forth below is the information required by paragraph 5.f.(1) of the Revised Supplemental Guidance for Conducting Computerized Matching Programs issued by the Office of Management and Budget (47 FR 21656; May 19, 1982.)"

- a statement indicating that a copy of the matching report has been provided to both houses of Congress and the Office of Management and Budget. This statement may be written as follows: "a copy of this notice has been provided both Houses of Congress and the Office of Management and Budget" (or) "a copy of this notice has been sent to the Speaker of the House, President of the Senate, and the Director of the Office of Management and Budget."

date signature

Report of Computer Matching Program

(a) Authority: The legal authority under which the match is being conducted;

(b) Program Description: A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose(s) for which the program is being conducted, and the procedures to be used in matching and following up on the "hits";

(c) Complete Description of Personal records including Federal Register citation where appropriate. A complete description of the personal records to be matched, including the source(s), system of records identifying data, date(s) and page number(s) of the most recent Federal Register full text publication where appropriate;

(d) Period of the Match: The projected start and ending dates of the program;

(e) Security: An appropriate description of the security safeguards to be used to protect against unauthorized access or disclosure of the personal records--the description shall not describe security safeguards in such detail that it increases the risk of unauthorized access to the records;

(f) Disposition of Records: Plans for disposition of the source records and "hits";

(g) Other Comments: This section should include any relevant pertinent information that is not included in other sections of the report.

OFFICE OF INSPECTOR GENERAL

COMPUTER APPLICATIONS
VOLUME I
HEALTH PROVIDER FRAUD AND ABUSE

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of Inspector General

Washington, D.C. 20201

Nearly a decade ago, a small headquarter's staff of auditors developed a unique computerized information retrieval system (HEWCAS) for the then Department of Health, Education, and Welfare. That "first small step" has led to today's breakthrough in computer applications designed to ferret out fraud, waste and abuse in the massive and myriad programs of the now Department of Health and Human Services.

Computer matching is a fast, efficient and accurate means to review voluminous amounts of data. Further, computer matches provide a major starting point in the detection and prevention of fraud, waste and abuse in expensive government programs.

As Inspector General of the Department of Health and Human Services, I am responsible for making more efficient an organization that is the largest distributor of funds in the Federal Government and whose annual budget is surpassed only by those of the United States and the Soviet Union. HHS spends over $250 billion annually on a variety of benefit, health service and research programs for the American people.

These range from Social Security, Medicare, Medicaid and Aid to Families with Dependent Children to the various health care and research programs of the Public Health Service.

Unfortunately, many of these vital programs are vulnerable to fraud, waste and abuse. The computer, therefore, has become a most important weapon in the crusade to make government more efficient and cost-effective.

We have made substantial investments in the Office of the Inspector General to recruit and develop the expertise to effectively and innovatively use high technology. Audit staff receive classroom exposure to EDP theory at our National Professional Development Center in Atlanta. And, each regional audit office is manned by staff with advanced EDP training.

Further, we operate within the strictures of the Privacy Act and the computer match guidelines established by the Office of Management and Budget.

More importantly, our expertise in computer matching is shared with those tasked with similar responsibilities -- at the Federal, State and local levels of government and now, with the private sector.

What follows is an up-to-date compendium -- for your use -- which dramatically illustrates some of our more successful computer applications to combat health provider fraud and abuse. We selected the health care area for our initial computer match series because of the massive expenditures involved. Our auditors have designed a number of computer programs that are tailored to isolate or quantify data in specific suspect areas. Other volumes, on other topics, will follow.

Hopefully, this initial compendium will be of assistance to those of you concerned with inefficiencies in the health care financing field. The concepts reviewed in this volume can be applied to many diverse areas. In fact, we believe the extent to which they are adaptable is limited only by the imagination of the user.

Additional information on these computer applications can be obtained by contacting our National Professional Development Center, 1365 Peachtree Street, N.E., (Suite 400), Atlanta, Georgia 30309, (404) 881-2891.

By working together and sharing our successes, we can make government at all levels more cost effective, the private sector more productive and insure that vitally-needed funds reach only those recipients for whom they were intended.

July 1982

Richard P. Kusserow
Inspector General
Department of Health and Human Services

VOLUME I

HEALTH PROVIDER FRAUD AND ABUSE

INVENTORY OF COMPUTER APPLICATIONS

OVERBILLING

I-1 PHYSICIANS

To identify billings from different physicians for the same type of service on the same day for the same patient.

I-2 PHYSICIANS

To determine whether physician billings were within the customary and prevailing rates for specific procedure codes.

I-3 PHYSICIANS

To identify physicians' billings for nursing home visits when a patient was not in a nursing home and to identify physicians' billings based on an individual rate when a reduced rate based on multiple visits was appropriate.

I-4 PHYSICIANS

To identify physicians' billings for services which should be covered under the methodone program.

I-5 PHYSICIANS

To identify instances where more than one surgeon billed for the same surgical procedures and instances where assistant surgeons billed at the same rate as the primary surgeon.

I-6 PHYSICIANS

To identify physicians who billed for a more extensive procedure than actually performed.

I-7 PROVIDERS

To identify claims for End Stage Renal Dialysis from "free standing facilities" which should be reduced when hospital services are provided on the same day.

I-8 PHARMACIES

To identify pharmacies who substituted brand name drugs with generic drugs when filling drug prescriptions but billed for the higher price brand name drug.

I-9 NURSING HOMES

To quantify the amount of claims for care of patients under 65 residing in nursing homes determined to be institutions for mental disease.

I-10 LABORATORIES

To identify billings for laboratory blood tests based on individual charges when a lower fee for multiple tests should have been used.

I-11 DURABLE MEDICAL EQUIPMENT

To identify delivery charges for durable medical equipment based on individual deliveries and to identify charges for durable medical equipment after date of patient death.

I-12 DURABLE MEDICAL EQUIPMENT

To identify billings for durable medical equipment when patients were in a health care facility responsible for providing the equipment.

DUPLICATE BILLINGS

I-13 PHYSICIANS

To identify duplicate physician billings for End Stage Renal Dialysis.

I-14 PHYSICIANS

To identify instances where the same or similar service is provided to one patient within a specific time frame and billed under more than one provider number.

I-15 PHYSICIANS

To determine whether a physician is billing for the same services under multiple provider numbers.

I-16 DENTISTS

To identify patients eligible for dental care under both a Prepaid Health Plan and a contract for dental services.

I-17 PROVIDERS

To identify fee-for-service payments when a patient was covered under a Prepaid Health Plan.

I-18 PROVIDERS

To validate the criteria used by processing systems to identify duplicate billings.

I-19 PROVIDERS

To identify providers with identification numbers in two contiguous geographic areas billing for the same patient services to both programs/plans.

I-20 PROVIDERS

To identify duplicate billings for out-patient services when the patient was in the hospital.

I-21 PROVIDERS

To identify duplicate billings by outpatient clinics and attending physicians working at the clinics.

I-22 LABORATORIES

To identify duplicate laboratory service billings for End Stage Renal Dialysis.

I-23 LABORATORIES

To identify duplicate billings for the same laboratory tests.

BILLINGS EXCEED NORMS

I-24 PHYSICIANS

To identify physicians whose number of prescriptions for classes of abuseable drugs exceed established norms.

I-25 PHYSICIANS

To identify physicians whose billings for specific medical procedures exceed established norms for one patient.

I-26 PHYSICIANS

To quantify overpayments to physicians which occurred because the number of billings for specific procedure codes exceeded specified limits for one patient.

I-27 DENTISTS

To identify dentists whose billings for specific dental procedures for one patient exceed established norms.

I-28 MEDICAL SPECIALISTS

To identify medical specialists, e.g. podiatrists, optometrists, and chiropractors whose billings for specific medical procedures exceed established norms for one patient.

I-29 PROVIDERS

To identify providers whose number of billings for unique/memorable services exceed the average number of times a patient would normally receive the services.

I-30 PHARMACIES

To identify pharmacies whose billings for specific prescription drugs exceed established norms for one patient.

I-31 PHARMACIES

To determine if the prescribed refill limits per patient on specific drugs were exceeded by dispensing prescriptions in the names of other family members.

I-32 PHARMACIES

To identify per patient billings from pharmacies which equal the maximum allowable monthly charge.

I-33 PHARMACIES

To identify pharmacies dispensing four or more prescriptions for abuseable classes of drugs within a 30-day period to one patient.

I-34 HOSPITALS

To identify, for certain diagnoses, hospital billings which exceeded length of stay parameters.

I-35 LABORATORIES

To identify laboratories whose billings for laboratory services for one patient exceeded established norms.

I-36 DURABLE MEDICAL EQUIPMENT

To identify medical equipment suppliers whose billings for specific items of equipment exceed established norms for one patient.

ILLOGICAL BILLING SITUATIONS

I-37 PHYSICIANS

To identify physician billings for inpatient hospital services when the patient was not in the hospital.

I-38 PHYSICIANS

To identify physicians' billings for laboratory services normally conducted in a hospital or clinic setting.

I-39 PHYSICIANS

To identify physicians' billings for initial visits which should be billed as subsequent visits with a lower rate.

I-40 PHYSICIANS

To identify billings for more than one abortion procedure within a short period of time.

I-41 PROVIDERS

To identify billings for sterilization related procedures for patients under 21.

I-42 HOSPITALS

To identify billings for outpatient services provided within 24 hours of an inpatient admission.

I-43 MEDICAL SERVICES

To identify billings for ambulance services where there were no medical services billed for that day or within one day.

I-44 MEDICAL SERVICES

To identify billings for blood administration charges when there was no corresponding billing for blood.

OVERBILLING - PHYSICIANS

Identified Vulnerability

Some health care plans limit the total number of times specific services, such as office visits, can be paid for one patient in one month. These limits should be based on the total of similar services provided rather than on the total number of different days the services were received. If the system does not accumulate statistics on situations where similar services are provided to the same patient on the same day from different physicians, an overbilling could occur.

OIG Action

A computer application was developed to identify billings for similar services provided on the same day to the same patient by more than one physician. The application also accumulated the total number of similar services provided in a month to one patient to identify overbillings and to illustrate the effectiveness of the controls in the claims processing system.

Results

The application was successfully run in one location. No problems with the controls in the claims processing system were noted.

OVERBILLING - PHYSICIANS

Identified Vulnerability

The lowest of the physician's actual charge, his customary charge or the area prevailing charge is normally the basis for reimbursement for services performed by physicians. The health care payment systems should contain edits to ensure that physicians are paid the appropriate rate for the service rendered. The concern is that when physicians bill at a rate higher than the area prevailing rate or the physician's customary charge, these higher charges may not be identified by the edit in the payment system.

OIG Action

To test the effectiveness of the payment edits for selected claims processing systems, the OIG developed computer applications to compare the amounts paid to physicians, for specified procedure codes, with the allowable amount for those codes. Differences would indicate the system screens are not effective or the edit controls are being by-passed.

Results

The application is in process; results are not yet available.

OVERBILLING - PHYSICIANS

Identified Vulnerability

Claims processing weaknesses could permit a physician to bill nursing home visits when a patient is not in a nursing home. In addition, a physician could overbill for nursing home visits. If a physician visits one patient in a nursing home, an individual rate is appropriate. If, however, a physician visits several patients, a reduced rate based on multiple visits is appropriate.

OIG Action

Applications were developed to compare physicians' claims with claims by nursing homes. A comparison, by date of service, will identify instances where a physician billed for visits when the patient was not in the nursing home. In addition, the application identifies instances when a physician visited more than one patient at the same home on the same day. For these identified instances, the physician's billing rate was validated and any overbillings were computed.

Results

The application was successfully run at one location. Over 26,000 claims totaling nearly $227,000 have been turned over to program administrators for follow-up.

OVERBILLING - PHYSICIANS

Identified Vulnerability

Under the methodone treatment program, patients receive physical screenings. These screenings, by physicians participating in the program, include checks of the patient's heart, lungs and blood pressure. For these services, the program pays the participating physicians an established fee for each encounter with the patient. If unusual symptoms are identified, patients can be referred to specialists for further diagnosis and treatment. Referral to outside physicians for routine screenings, however, would result in overbilling for services and could indicate potential abuse of the program.

OIG Action

A computer application was developed to identify billings from outside physicians for routine screenings of methodone patients.

Results

Billings for routine screenings of 3900 methodone patients were identified. The overbillings at this one location amounted to about $250,000.

OVERBILLING - PHYSICIANS

Identified Vulnerability

Some medical procedures may require more than one physician to be in attendance. For example, a surgical procedure may require, in addition to the surgeon, the services of an assistant surgeon and an anesthesiologist. In other situations a particular diagnosis may require the services of more than one physician. Each physician should be reimbursed for the services actually rendered as part of the concurrent care. The amount reimbursed would depend on the type of service rendered.

When several physicians are involved in delivering a similar medical service the procedure code used for billing by each physician should reflect the service actually performed. For example, a doctor acting as an assistant in surgery should not bill as the surgeon in attendance. Nor should two physicians bill for the same service. These situations would result in overpayments for services actually rendered. Claims processing systems may not have controls designed to detect these types of overbillings.

OIG Action

A computer application was developed to identify situations where it appeared that physicians (1) were billing for the same service, (2) were billing for services which were not actually rendered, or (3) were billing for a procedure code which would have resulted in being reimbursed at a higher rate than the rate allowed for the service actually performed.

Results

The application was run in one location. Approximately $100,000 in overpayments were identified.

OVERBILLING - PHYSICIANS

Identified Vulnerability

Physicians receive payment for their services based on procedure codes. The billing rate for each procedure code is based on the complexity of the medical service or the length of time needed to give the medical treatment. An annual physical examination, for example, will take more time and be billed at a higher rate than a short office visit.

To maximize reimbursement from health care programs, physicians could bill for procedure codes identifying more complex or lengthy procedures than actually performed. These billings could be for medical care provided in the physicians office, a hospital, a nursing home, or a patient's home.

OIG Action

A computer application was designed to identify selected medical procedures billed by physicians for care given to patients in the office, hospital, nursing home, or the patient's home. The procedures selected were the more extensive and complex types of care which, under normal medical practices, a patient would receive infrequently.

Results

The application was run in one location. Edit controls in the computer system did not detect frequent billings for complex medical procedures. Results of the application were turned over to program administrators. Overbilling of almost $500,000 have already been repaid.

OVERBILLING - PROVIDERS

Identified Vulnerability

Services for End Stage Renal Dialysis may be provided by a "free standing facility" or by a hospital. An in-patient in the hospital may also receive services from the free standing facility on the same day. However, the rate to be billed for the services is not the same. Without controls in the claims processing systems to identify the different "sources" of the services and reduce the billing rate, billings could be overstated.

OIG Action

A computer application was developed to match billings from the free standing facilities and hospitals on the same date for the same patient.

Results

Application in process. Results not yet available.

OVERBILLING-PHARMACIES

Identified Vulnerability

Pharmacies are paid for prescriptions based on the drug code billed. Reimbursement under a brand name drug code is generally significantly higher than under a generic drug code. When pharmacies bill for reimbursement, the dispensed drug is coded on the claim. The payment system computes the reimbursement based on the drug code billed. If a generic drug was used to fill a prescription and the brand name code was used on the billing, the pharmacy would be reimbursed at the brand name (higher) rate. Most payment systems are not designed to detect this type of overbilling.

OIG Action

Prescription drugs were identified that (1) are extensively used, (2) are available in both the brand name and the generic form, and (3) are cheaper in the generic form. A computer application was developed to identify pharmacies whose preponderance of billings were for brand-name drug codes.

Results

Application is in process; results are not yet available.

OVERBILLING -- NURSING HOMES

Identified Vulnerability

The Federal Government does not participate in the cost of care and treatment for patients under 65 in an institution for mental diseases. In some instances, intermediate or skilled nursing facilities are, in fact, institutions for mental diseases and should not be eligible for Federal funding for costs related to patients under 65.

OIG Action

Data on nursing home facilities was reviewed to identify those homes operating as institutions for mental diseases. A computer application was developed using the payment history for those identified nursing homes to calculate patient days and costs associated with care for patients under 65 years of age.

Results

The application was run for five locations. Two million three hundred thousand dollars is the estimated amount of overbilling.

OVERBILLING - LABORATORIES

Identified Vulnerability

Laboratories perform over twenty-six blood chemistry procedures and complete blood count tests. Since individual procedures may be requested, each procedure has an identified billing rate. However, if numerous procedures are requested using the same blood sample, generally the first procedure will be billed at a specific rate and all additional procedures at a greatly reduced rate. If the laboratory billed for each procedure at the higher individual rate, the health care programs would be significantly overbilled. It is, therefore, important to have edits in the payment systems to identify these potential overpayments.

OIG Action

A computer application was designed to analyze payments for blood chemistry procedures and complete blood count tests performed on the same date. For those identified instances the billing rate was validated and any overbillings were computed.

Results

This program was run at one location. Seventy-eight thousand dollars in overpayments were refunded.

OVERBILLING - DURABLE MEDICAL EQUIPMENT

Identified Vulnerability

Several types of claims have been identified as having significant potential for overbilling. In the area of durable medical equipment, we identified two scenarios which warranted review: (1) billing for individual deliveries when lower cost route deliveries were made, (2) billing for services after the patient died.

OIG Action

In durable medical equipment, we isolated deliveries of oxygen by a number of providers to the same geographic area. We developed a computer application to list all providers who billed for individual deliveries in the same area for the same day, but for different patients.

We also compared billings for durable medical equipment with a tape listing all deaths for a specific period.

Results

The applications were run at two locations. Overbillings by 15 providers were identified and turned over to program administrators for action.

OVERBILLING - DURABLE MEDICAL EQUIPMENT

Identified Vulnerability

When patients are residing in nursing homes, charges for durable medical equipment should be included as part of the per diem paid to the nursing home. However, in some instances suppliers are also billing for providing durable medical equipment to the same patients. This potential for overbilling exists because the computerized file does not accurately reflect the "place of service."

OIG Action

Computer applications were designed to identify the location of the patient when the supplier billed for the durable medical equipment. This identification was accomplished by comparing the dates of billing with the dates the patient was in the nursing home.

Results

Potential overpayments of about $1.4 million were identified.

DUPLICATE BILLINGS - PHYSICIANS

Identified Vulnerability

Physician services for End Stage Renal Dialysis can be billed through two different claims processing systems. One system processes all billings for services from a group practice called a "free standing facility" using the facility's identification number. The other system processes billings from physicians using their individual identification number. Thus, the same services could be billed twice.

OIG Action

A computer application was developed to match billings with different identification numbers for the same patient on the same day.

Results

The application is in process. Results not yet available.

DUPLICATE BILLINGS - PHYSICIANS

Identified Vulnerability

Many physicians participate in group practices. One billing problem resulting from this arrangement is called tandem billing. That is, several physicians in the same group bill for similar services provided to the same patient within a short time frame. These billings are submitted under the individual identification numbers of the various physicians. Tandem billing, of course, is not limited to group practices. Claims processing systems may not have edits to identify instances of duplicate billings for the same or similar services by more than one physician.

OIG Action

A computer application has been developed to identify billings for the same or similar service within a short time frame by more than one physician.

Results

The application has been run in four locations. An estimated $200,000 in duplicate payments have been identified for recovery.

DUPLICATE BILLINGS - PHYSICIANS

Identified Vulnerability

Health care programs allow physicians to have more than one provider identification number. The same physician could have one number as an individual provider and another number as a member of a group practice. The same physician could also have additional numbers--one assigned to each office the physician maintains. Present controls in the claims processing systems may not assure detection of billings for the same services submitted under more than one provider identification number.

OIG Action

Computer applications are being developed to identify physicians who have more than one provider identification number. After a reference file is developed, comparisons will be made with paid claims files.

Results

Application is being developed. After testing, the application will be run at two locations.

DUPLICATE BILLINGS - DENTISTS

Identified Vulnerability

Dental services are available to patients under two plans - a Prepaid Health Plan (PHP) and a contract. Participants in the PHP are required to obtain all services under the plan, since the plan is reimbursed on a per person basis rather than individual billings for services. Services provided under the contract are paid on a billing for services basis. With separate claims processing systems for each plan, a participant in the PHP could receive and billing could be made for dental services under the contract. No controls are in place to compare PHP enrollment with billings for dental services under the contract.

OIG Action

Computer data from both processing systems were compared to identify patients who were eligible for dental services under a PHP but receiving these services under a contract.

Results

The application was run at one location. Because internal controls were not in place to compare PHP eligibility data with contractor billings, excess payments of $287,000 were made.

DUPLICATE BILLINGS - PROVIDERS

Identified Vulnerability

A health care program offers two options for coverage. One is enrollment in a Prepaid Health Plan (PHP); the other one is on a fee-for-service basis. Without proper internal controls in the payment systems, the health care program could be paying twice for the same services. This problem would be compounded if accurate and timely adjustments were not made for changes in eligibility.

OIG Action

A computer application was developed to compare payments made to patients under both plans, within a specific time frame.

Results

The application was run at two locations. To date, adjustments of $12 million of duplicate payments have been targeted for recovery, another $9.6 million of adjustments are in the review stage and an additional $237,000 has been identified for follow-up action.

DUPLICATE BILLINGS - PROVIDERS

Identified Vulnerability

The computerized claims processing system has edits to detect duplicate billings. However, there are a number of criteria which must be matched before a duplicate claim can be identified. If the criteria is very restrictive, such as paid-date matching, many duplicate claims will not be identified.

OIG Action

Using less restrictive criteria, a computer application was developed to review claims processed during a one year period for potential duplicate billings.

Results

A review of 308,236 claims at one location identified 3441 claims which had been paid more than once. The matching criteria used in our computer application have been incorporated as edits in the computerized claims processing system.

DUPLICATE BILLINGS -- PROVIDERS

Identified Vulnerability

Claims processing systems cover billings from defined geographic areas. Identification numbers are issued for providers offering and billing for services provided in that geographic area. If a provider serves contiguous geographic areas, a separate identification number would be issued for each area. This situation allows the same services for the same patient to be billed through two claims processing systems, using the identification number applicable to each system.

OIG Action

A computer application was developed to compare billings for the same services on the same dates for the same patient and processed through the different systems serving contiguous areas.

Results

Application is in process. Results are not yet available.

DUPLICATE BILLINGS -- PROVIDERS

Identified Vulnerability

Because claims for outpatient services and inpatient services are billed separately, the possibility for duplicate billings exist. That is, billings for services as an inpatient could duplicate billings for the same services either (1) as an outpatient prior to admission as an inpatient, or (2) as an outpatient while the patient is a full-time inpatient. The claims processing system may not have the capability to identify claims where dates and types of service match.

OIG Action

A computer application was developed to identify billings for outpatient services on (1) the same dates billings were made for inpatient services, or (2) the same dates services were included in the inpatient per diem rate.

Results

At one location, for a 24-month period, duplicate claims totaling $3.5 million were identified.

DUPLICATE BILLINGS - PROVIDERS

Identified Vulnerability

Many attending physicians at outpatient clinics maintain a private practice, in addition to their work at the clinics. As such, the physicians have an individual provider identification number for billing for services provided as part of their private practice. This individual identification number could be the source of duplicate billing. That is, the physicians services provided at and billed by the clinics could also be billed as services provided as part of their private practice.

OIG Action

A computer application to identify billings for the same services on the same day for the same patient from both a clinic and a physician was developed.

Results

Application is in process. Results not yet available.

DUPLICATE BILLINGS - LABORATORIES

Identified Vulnerability

Laboratory services for End Stage Renal Dialysis may be billed by two different methods resulting in possible duplicate billings. A "free standing facility" may bill for a laboratory service, use a general procedure code and bill under the facility's identification number. The laboratory providing the service may bill under a different identification number and use a specific procedure code. Controls in the systems may not identify these two billings as duplicates.

OIG Action

A computer application was developed to match billings processed under both procedures. Specifically, the claims for the same patient for the same day will be matched.

Results

The application is in process. Results not yet available.

DUPLICATE BILLINGS - LABORATORIES

Identified Vulnerability

Laboratory tests are necessary procedures in patient diagnosis. Some laboratory tests can be conducted in the physicians offices, while other more sophisticated tests may be conducted by outside laboratories. Since billings from the physicians and from the laboratories use different provider identification numbers, the possibility of duplicate payments exists.

OIG Action

Computer applications were developed to identify billings from physicians and laboratories on the same day for the same patient.

Results

The application was run in five locations. Billings in excess of $1 million dollars have been referred to program administrators for follow-up.

BILLINGS EXCEED NORMS -- PHYSICIANS

Identified Vulnerability

Health care programs, designed to provide needed services, offered opportunities for overutilization and billings exceeding acceptable norms. For example, physicians could prescribe excessive dosages of drugs. This practice is especially critical if the prescriptions are for abuseable drugs.

OIG Action

With the help of medical and pharmacological professionals, individual and classes of abuseable drugs were identified and normal dosages established. A computer application was designed to identify physicians whose prescriptions to one patient exceeded established norms.

Results

The application was run at one location. Results were turned over to program administrators for follow-up.

BILLINGS EXCEED NORMS -- PHYSICIANS

Identified Vulnerability

Physicians provide a wide variety of medical services reimbursed under the health care programs, both those services provided for continual care and those services of a non-recurring nature. The number of billings for procedures for continual care or procedures for non-recurring treatment may exceed the number of times a procedure would normally be provided.

OIG Action

With assistance from program administrators and medical professionals, parameters for 22 medical procedures were established and the "norm" for the number of times each procedure would be performed on one patient within one year established. A computer application was developed to compare these norms with physician billings.

Results

The application was run nationwide, resulting in system changes in the claims processing and utilization review systems. Overpayments totaling $6.8 million were identified for further review.

BILLINGS EXCEED NORMS -- PHYSICIANS

Identified Vulnerability

Some health care programs establish a maximum number of times a single provider can be reimbursed for the same medical procedure within a given period of time. If the claims processing systems do not have edit capabilities which will identify the claims exceeding the established limit for a particular procedure code, excessive costs to the program may result.

OIG Action

Procedure codes which have maximum usage limits were identified. An application comparing physician billings with established limits was developed.

Results

The application was run in two locations and resulted in identified overpayments of $452,000. The application is presently being run in a third location.

BILLINGS EXCEED NORMS -- DENTISTS

Identified Vulnerability

Under the health care programs some dental care is mandatory. For persons under 21, a minimum amount of dental care necessary for the relief of pain and infection and restoration of teeth must be provided. Dental care for other participants in the program is an optional service. Program services required for persons under 21 could result in billings exceeding acceptable norms.

OIG Action

Using guidelines established by the programs and recommendations from dental providers, limits were defined for selected dental services. A computer application was developed to compare dentists' billings with established limits. Additionally, the application compares dentists' billings with billings from others in his peer group.

Results

The application was run in six locations. Weaknesses in internal control and utilization review systems were identified and referred to program administrators for corrective action.

BILLINGS EXCEED NORMS -- MEDICAL SPECIALISTS

Identified Vulnerability

Medical specialists, such as podiatrists, optometrists, and chiropractors, provide specialized services covered by the health care programs. Although the services are nontraditional, the providers could be billing for services that were not provided or for services provided more frequently than would generally be needed by a patient.

OIG Action

Limitations were developed for 26 procedures or groups of procedures that are associated with medical specialists. The limitations were compared with the actual billings from medical specialists.

Results

The application was run at two locations. The results were referred to program administrators for further review.

BILLINGS EXCEED NORMS -- PROVIDERS

Identified Vulnerability

A few providers in all health care programs intentionally submit billings for services that they did not provide patients, billings for more extensive and costly services than those provided, or billings for providing services more frequently than needed.

OIG Action

Using Departmental medical specialists, specific medical procedures that were unique and memorable in nature were identifed. The types of procedures included those which were painful for the patient, those so specialized that it required total physician participation, those which were extremely lengthy in nature, or those which would normally be done once a year. An application was developed to identify excessive billings from providers for any of these medical procedures.

Results

The application was run in several locations. Results were referred to investigative authorities.

BILLINGS EXCEED NORMS -- PHARMACIES

Identified Vulnerability

Some claims processing systems process billings for prescription drugs by patient identification number. Because pharmacies have access to the patient's identification number, billings can be submitted for more drugs than were prescribed or for drugs that were not prescribed.

OIG Action

The maximum number of prescriptions and dosage for 26 drugs and drug groups were identified. A computer application compared these maximums to the total number of prescriptions filled for one patient in one year.

Results

The application, run at several locations, showed weaknesses in controls in processing systems and weaknesses in controls relating to monitoring the health care programs.

BILLINGS EXCEED NORMS -- PHARMACIES

Identified Vulnerability

Health care programs have established controls to minimize the misuse of prescription drugs. For example, a limit on the number of prescriptions per patient has been established. However, this control can be circumvented by dispensing the same drug in the names of other family members, as well as dispensing the same drug by both brand name and generic name.

OIG Action

A computer application, using family rather than individual identifier, was developed to identify excessive dispensing of specific drug codes.

Results

The application was run at one location. Results were referred to investigative authorities.

BILLINGS EXCEED NORMS -- PHARMACIES

Identified Vulnerability

One of the controls established by health care programs for drug administration is a limit on the total dollar amount paid monthly for drugs for one patient. Pharmacies could, however, be billing at or near the dollar limit rather than for the actual dollar amount of the prescriptions dispensed. Billings which exceed the dollar limit must have prior physician approval.

OIG Action

A computer application was developed to identify pharmacies where a majority of the billings were at or near the monthly dollar limit.

Results

The results of the application, run at one location, were referred to investigative authorities,

BILLINGS EXCEED NORMS -- PHARMACIES

Identified Vulnerability

Controls are normally designed to identify excessive dispensing by pharmacies of individual drugs rather than of classes of drugs. These controls can, therefore be circumvented by dispensing multiple abuseable drugs in the same drug class.

OIG Action

A computer application was developed to identify billings for four or more prescriptions within a 30-day period to one patient of any of eight classes of abuseable drugs.

Results

The results of the application, run at one location, were referred to program administrators for action.

BILLINGS EXCEED NORMS -- HOSPITALS

Identified Vulnerability

Length of stay at hospitals for similar illnesses should be fairly consistent and within parameters established by health care professionals. Excessive billings from hospitals may indicate overutilization of the services provided by the health care program.

OIG Action

A computer application was developed to list billings exceeding the parameters established by medical societies and program administrators.

Results

This application, run at two locations, identified hospitals consistently exceeding established parameters. The listing was referred to program administrators for action.

BILLINGS EXCEED NORMS -- LABORATORIES

Identified Vulnerability

Excessive costs to the health care program can result from billings for laboratory tests that were (1) performed and billed more frequently than needed, or (2) billed and not performed.

OIG Action

Medical specialists established parameters for the number of times within an established period routine laboratory tests would normally be administered to one patient. These norms were compared to actual laboratory billings.

Results

The application was run at five locations. Overpayments exceeding $1.6 million were identified and referred to investigative organizations and program administrators.

BILLINGS EXCEED NORMS -- DURABLE MEDICAL EQUIPMENT

Identified Vulnerability

Like other medical services paid under the health care programs, billings for durable medical equipment for one patient can exceed established norms.

OIG Action

An application was designed to compare billing practices by various suppliers within geographic areas and to identify billings for types of equipment supplied more frequently than would normally be used.

Results

Billings for almost 15 percent of the providers of durable medical equipment were identified as having had exceeded the established norms and referred to program administrators for action.

ILLOGICAL BILLING SITUATIONS -- PHYSICIANS

Identified Vulnerability

Health care programs processed physicians' billings for inpatient visits separately from hospital billings for services. For the physician billings for inpatient visits to be valid, the patient must be confined to the hospital for the dates services were provided. Since these two billings are processed through different systems, edits may not be in place to identify incompatible charges.

OIG Action

A computer application was developed to compare the dates of the physicians' visits with the dates of the inpatient charges.

Results

The application was run in one location. Weaknesses in the claims processing activities were identified.

ILLOGICAL BILLING SITUATIONS -- PHYSICIANS

Identified Vulnerability

Physicians, as part of their office services, perform and bill separately for laboratory tests conducted in their offices. There are some tests, however, that are unique in nature, thus normally requiring a hospital or clinical setting. Charges for these tests would not normally be billed by the physician. Because laboratory tests are a normal element of the physicians' billings, claims processing systems may not have edits to isolate claims for unique laboratory tests.

OIG Action

Laboratory tests normally performed in a hospital or clinical setting were identified. Billing codes for these tests were matched with physicians' billings to identify illogical claims.

Results

The application was run in five locations. Billings totaling $510,000 were referred to program administrators for follow-up.

ILLOGICAL BILLING SITUATIONS -- PHYSICIANS

Identified Vulnerability

Physicians must spend more time with patients during the initial office visit than subsequent visits during the year. Recognizing this, different billing codes and different rates are used for initial office visits and subsequent visits. The claims processing system, however, may not have edits which will identify visits incorrectly coded as initial visits and billed at the higher rate.

OIG Action

A computer application was developed to verify the edits which identify multiple billings for a specific procedure code.

Results

The application, run at one location, has identified over $500,000 in excessive payments.

ILLOGICAL BILLING SITUATIONS -- PHYSICIANS

Identified Vulnerability

Some medical procedures covered by health care programs are not frequently administered within a short period of time. An abortion procedure is one of these specialized services. Claims processing systems may not have edits designed to identify recurring claims for procedures which are infrequent in nature.

OIG Action

A computer application was designed to identify billings for the abortion procedure code where more than one claim was processed within a short period of time.

Results

The program was run in one location. The results were turned over to program administrators for follow-up.

ILLOGICAL BILLING SITUATIONS -- PROVIDERS

Identified Vulnerability

Although health care programs allow charges relating to sterilization, the patient must be over 21 years old. Providers could bill for sterilization procedures and related services if controls in the claims processing system did not segregate billings for persons under 21.

OIG Action

A computer application was designed to identify claims for sterilization and related services.

Results

Five hundred sterilization and related service claims were identified. The claims totaling over $300,000 were referred to program administrators for follow-up.

ILLOGICAL BILLING SITUATIONS -- HOSPITALS

Identified Vulnerability

Billings for outpatient services provided within 24 hours of an inpatient admission at the same hospital should be included in the billings for hospital services. The claims processing system for hospital billings may not include procedures to identify incorrect claims.

OIG Action

A computer application was developed to compare outpatient and inpatient files to detect incorrect claims.

Results

At one location, for a 12-month period, over 12,000 claims were identified as improper and referred to program administrators for review.

ILLOGICAL BILLING SITUATIONS -- MEDICAL SERVICES

Identified Vulnerability

Claims for certain types of medical services should have other related claims within the same or following day. One example is ambulance service. If a patient requires the service of an ambulance, it is logical that additional medical services will be administered and billed. Edits may not be in place to verify the related procedure codes to ensure the validity of billing for ambulance services.

OIG Action

A computer application was developed to list billings for ambulance services with no corresponding claims for medical service for claims on the same or subsequent day.

Results

The application is in process. Results are not yet available.

ILLOGICAL BILLING SITUATIONS -- MEDICAL SERVICES

Identified Vulnerability

Billings for certain types of medical procedures should always be related. For example a billing for blood administration should always have a corresponding billing for the blood. The claims processing system may not include a procedure for comparing the corresponding blood administration and blood billings.

OIG Action

The billings for blood and blood administration were matched through a computer application.

Results

At one location, the application identified over 2,300 blood administration claims amounting to $112,000 with no corresponding claims for blood.

DEPARTMENT OF HEALTH & HUMAN SERVICES-USA

OFFICE OF INSPECTOR GENERAL

COMPUTER APPLICATIONS

VOLUME II

INCOME MAINTENANCE AND ASSISTANCE FRAUD AND ABUSE

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of Inspector General

Washington, D.C. 20201

As Inspector General of the Department of Health and Human Services, I am committed to ferreting out fraud, waste and abuse in the massive and myriad programs of the Department. To identify potential problems in the programs, my staff has designed a number of computer applications. The computer applications, operated within the strictures of the Privacy Act and the computer match guidelines established by the Office of Management and Budget, are tailored to quantify specific identified vulnerabilities.

Some of our more successful computer applications, designed to combat health provider fraud and abuse, were published in July 1982.

This, our second volume, summarizes 17 computer applications designed to highlight illogical entitlement and invalid eligibility situations in the income maintenance and assistance programs.

Although these computer applications were tailored to meet specific objectives, they may be applied to many diverse, but related, situations. In fact, we believe the extent to which they are adaptable is limited only by the imagination of the user.

Maximum benefits from the results of these applications can only be accomplished by sharing with those tasked with similar responsibilities at the Federal, State and local levels of Government.

By working together and sharing our successes, we can make government at all levels more cost effective and insure that vitally-needed funds reach only those recipients for whom they were intended.

September 1982

Richard P. Kusserow
Inspector General
Department of Health and
Human Services

COMPUTER APPLICATIONS

VOLUME II

PREFACE

The Inspector General of the Department of Health and Human Services is responsible for making more efficient an organization that is the largest distributor of funds in the Federal Government and whose annual budget is surpassed only by those of the United States and the Soviet Union. HHS spends over $250 billion annually on a variety of benefit, health service and research programs, ranging from Social Security, Medicare, Medicaid and Aid to Families with Dependent Children to the various health care and research programs of the Public Health Service.

Unfortunately, many of these vital programs are vulnerable to fraud, waste and abuse. The computer, therefore, has become a most important weapon in the crusade to make government more efficient and cost-effective.

Computer applications are an efficient and accurate means to review voluminous amounts of data. Further, the results provide a major starting point in the detection and prevention of fraud, waste and abuse in expensive government programs.

The Office of Inspector General has made substantial investments to recruit and develop the expertise to effectively and innovatively utilize computer technology. A unique computerized information retrieval system (HEWCAS), classroom exposure to EDP theory at our National Professional Development Center in Atlanta, and regional audit offices manned by a staff with advanced EDP training provide the resources to develop innovative computer applications.

Some of these are summarized in this compendium. Additional information on these computer applications can be obtained by contacting the National Professional Development Center, 1365 Peachtree Street, NE., Suite 400, Atlanta, Georgia 30309, (404) 881-2891.

VOLUME II

INCOME MAINTENANCE AND ASSISTANCE FRAUD AND ABUSE

INVENTORY OF COMPUTER APPLICATIONS

ILLOGICAL ENTITLEMENT SITUATIONS

II-1	To identify instances where unissued or illogical social security numbers were used in entitlement programs.
II-2	To identify checks paid from entitlement programs which had not been cashed within 90 days of issuance.
II-3	To identify payments by entitlement programs after date of death.
II-4	To identify instances where multiple payments were sent to the same post office box.
II-5	To identify instances where the total number in the family unit may have included children who did not exist.
II-6	To identify instances where individuals may have been claimed as members of more than one family unit.
II-7	To identify instances where auxiliary assistance payments were made for purposes other than to remedy underpayments occurring in a month of a permanent change in status.
II-8	To identify instances where divorce or death terminated payments for some, but not all, entitlement programs.
II-9	To identify "worst-case" instances where illogical or invalid support was used by individuals in qualifying for entitlement programs.

INVALID ELIGIBILITY SITUATIONS

II-10 To identify instances where Federal employees were participating in assistance programs.

II-11 To identify instances where benefit payments were made to children or students who exceeded the statutory age limit for eligibility.

II-12 To identify instances where an individual was participating in the same assistance program in more than one jurisdiction.

II-13 To identify instances where payments were made to the same individuals by two mutually-exclusive assistance programs.

II-14 To identify instances where vendor payments, as part of an assistance program, were made for individuals who were ineligible.

II-15 To identify instances where identical social security numbers were being used for more than one active case in the same assistance program.

II-16 To identify instances where significant amounts of earned income were not reported, and thus not considered, in determining eligibility for an assistance program.

II-17 To identify instances where current eligibility status was not used in recomputation of program benefits.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Social security numbers (SSN's) are frequently used as individual identifiers in entitlement programs. Unissued or illogical SSN's could indicate (1) inaccurate data is being used to determine eligibility or to compute benefits, (2) systems controls need to be strengthened, or (3) potential for fraud or abuse in the entitlement programs.

OIG Action

The range of valid SSN's was obtained from the Social Security Administration. A computer application was developed to screen the SSN's and print exceptions.

Results

The application was successfully run at ten locations. Additionally, several state agencies have been furnished copies of the application.

Identified exceptions have ranged from 800 SSN's at one location to 23,000 SSN's at another location. In one location, the application identified 5,000 SSN's that had not been issued by SSA.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Checks paid for entitlement programs are normally cashed within a short time after receipt. Checks being held for extended periods (over 90 days) could indicate potential problems.

OIG Action

A computer application was developed to list checks outstanding for more than 90 days.

Results

The application is in process; results not yet available.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Payments under entitlement programs are either terminated or recomputed for dependents when a primary beneficiary of the program dies. It is, therefore, essential the information on date of death is input to the master records. If this action is not taken timely, the results can be overpayments or payments to ineligible individuals.

OIG Action

A computer application was developed to compare death records with the payment records from various entitlement programs. Listings of payments to primary beneficiaries after death were listed.

Results

The application was successfully run at seven locations. Improper payments of over $300,000 involving more than 250 cases have been identified.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Checks from the same entitlement program addressed to a post office box may indicate duplicate payments or other improper payment situations.

OIG Action

A computer application was developed to list all post office boxes to which two or more checks were delivered.

Results

Application still in process; results not yet available.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Computation for payments from some entitlement programs are based on the total number of members in the family unit. That is, the larger the family unit, the greater the amount of program payment. If children who do not exist were included as part of the family unit, overpayments would occur.

OIG Action

The OIG staff designed a computer application to match the entitlement file with the health care paid claims file. In designing the application, the premise was that eligible children of school age would be expected to have received medical services within a two-year period.

Results

The application was successfully run at one location. There were 755 cases identified where children had not received medical services. Review of the 755 cases is on-going. To date, 52 cases have been referred to investigative authorities.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Income maintenance and assistance programs provide benefits to family units. However, an individual can only be a member of one family unit. For example, children who live with a mother or grandmother cannot be included in another family unit formed by the father. Using different last names, the same individual could be listed as part of more than one family unit and thus be participating in benefits from the programs more than once.

OIG Action

A computer application was developed to identify situations where there was a high probability individuals were participating in program benefits more than once. The application matched the first names and birthdays of two individuals in one case with the first names and birthdays of two individuals in other cases.

Results

The application has been successfully run at six locations. At one location 59 instances with about $400,000 in overpayments were identified. Results from the five other locations identified 103 additional cases. These cases are being reviewed.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

Auxiliary checks are issued when there is a permanent change in status and the caseworker is not notified in time to increase the regular check. The use of auxiliary checks is a one-time remedy, with regular checks which follow reflecting the permanent change. If controls are not fully implemented, auxiliary checks could be issued for other than the intended purpose.

OIG Action

A computer application was developed to compare the auxiliary payments with the regular payments. The resulting list included (1) instances where the regular check for each of the two months following the auxiliary payment did not reflect the permanent change, and (2) instances where no regular check was issued during the month of or the month following the auxiliary payment.

Results

The application was successfully run at one location. Results were turned over to the investigative authorities for review.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

In instances where beneficiaries received benefits from more than one program, changes in status reported to one program may not be reflected in another program. For example, spouses and widows may be receiving benefits from the Social Security Title II program and from the Black Lung program. Through divorce or death, the spouses and widows may have been removed from eligibility for Title II. However, the procedures may not have been adequate to ensure these changes in status were reported to the Black Lung program.

OIG Action

A computer application was developed to compare the spouses and widows receiving benefits under the Black Lung program with the master beneficiary records of the Title II program.

Results

The application identified 1,209 cases of possible overpayment of Black Lung Benefits. Further review identified 829 cases requiring both termination action and action to recoup over $4.6 million in overpayments. Additionally, weaknesses in systems controls were identified.

ILLOGICAL ENTITLEMENT SITUATION

Identified Vulnerability

One of the most significant problems with the income maintenance and assistance programs is the possibility of payments to ineligibles and overpayments to eligibles. Each type of scenario can be developed and appropriate computer applications developed to identify the problems. However, it is especially important to identify the "worst case" situations resulting from more than one type of program deficiency.

OIG Action

A computer screen has been developed to combine several applications. The resulting listing identifies those cases which repeatedly turn up when matching for (1) duplicate social security numbers, (2) invalid social security numbers, (3) eligibility in more than one jurisdiction, and (4) eligibility after change in status (divorce or death).

Results

The screening concept has been successfully run at one location. Initial results are being reviewed.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

The income maintenance and assistance programs are primarily designed to assist those individuals who are economically deprived. Especially during this austerity period, it is important to provide benefits to only those who are eligible. With emphasis on ferreting out fraud and abuse, it is especially important not to have Federal employees receiving benefits if they are not eligible.

OIG Action

Computer applications were developed to compare payroll data from Federal agencies with benefit payment files.

Results

The application has been successfully run. To date, over $212,000 in overpayments have been identified; some payments were made to ineligibles. Additional applications have been run and results referred to appropriate Federal and State program administrators.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

Under the Black Lung program, children are eligible to receive benefits up to age 18 or, if students, up to age 23. To preclude overpyaments, the program needs controls to identify the children reaching the cut-off age and stop the benefit payments.

OIG Action

A computer application was developed to screen the benefit files for any child or student who had reached the statutory age limits and was still receiving benefits.

Results

The application was successfully run. About 3,000 children were identified who were possibly ineligible for benefit payments. Subsequent review of the 3,000 cases disclosed 1,426 ineligible recipients and $1.6 million in overpayments.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

Income maintenance and assistance program regulations preclude individuals from receiving benefits from more than one jurisdiction during the same period. However, the programs are usually the responsibility of different administrations in different jurisdictions. Usually there are no controls to compare the eligibility data in different jurisdictions to preclude duplicate payments for benefits.

OIG Action

A computer application was developed to compare the eligibility files in different jurisdictions and to identify any duplicate enrollments.

Results

The application was successfully run in 44 locations. To date, over 6,000 possible duplicate enrollments have been identified and turned over to program officials for review.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

In some instances, income assistance programs specifically prohibit the payment of concurrent benefits. For example, the State administered program for foster care precludes payments under the Federally administered program. Without sufficient controls to compare eligibility and payments, improper payments could occur.

OIG Action

A computer application was developed to compare eligibility and payment records of both programs.

Results

The application was successfully run at one location. Some instances of potential duplicate payments were referred to program administrators for follow-up. New controls have been implemented in the State administered program to detect future occurrences.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

As part of an income assistance program, payments for rent or a mortgage are made directly to vendors. The vendor payment system is separate from the related system for support payments. Therefore, vendor payments could be made when the individual is not eligible.

OIG Action

A computer application was developed to compare the eligibility file with the vendor payment file.

Results

The application was successfully run at one location. Improper payments totalling about $400,000 were identified.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

Individuals applying for benefits from income maintenance and assistance programs use their social security number as an identifier. Overpayments can occur if (1) the individual was receiving benefits but reapplied in the same jurisdiction using the same social security number and was being paid under both applications or (2) the individual using the same social security number, applied and was paid benefits in more than one jurisdiction.

OIG Action

A computer application was developed to compare date of birth and social security number of eligible individuals to identify those on the file more than once. Another application compared date of birth and social security number of eligible individuals to identify those on files in different jurisdictions.

Results

The application was successfully run at three locations. At one location an individual was identified who had received $330,000 in overpayments. Results from the two other locations are not yet available.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

Income maintenance and assistance programs usually consider income from individuals in determining eligibility. If an individual does not report earnings or unemployment compensation they are receiving, either when they apply for benefits or when they are participating in the program, overpayments may occur.

OIG Action

A computer application was developed to compare earnings records and unemployment records with the active assistance files.

Results

The application is in process; results are not yet available.

INVALID ELIGIBILITY SITUATION

Identified Vulnerability

In some situations, individuals are eligible to receive benefits from both a Federally administered program and a State administered program. The benefit computations for the programs are related. That is, an individual being removed from the State administered program would receive more benefits from the Federally administered program.

Notification of removal from the State administered program without the subsequent actual removal of the individual results in overpayment of benefits from the Federally administered program.

OIG Action

A computer application was developed to identify individuals receiving benefits from the Federally administered program who were originally also receiving benefits from the State administered program.

Results

The application was successfully run in one location. Cases involving individuals who had been receiving benefits from both programs were reviewed. Overpayments exceeding $1 million were identified.

OFFICE OF INSPECTOR GENERAL

COMPUTER APPLICATIONS

VOLUME III

FEDERAL AND STATE PROGRAMS FRAUD AND ABUSE

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of Inspector General

Washington, D.C. 20201

As Inspector General of the Department of Health and Human Services, I am committed to ferreting out fraud, waste and abuse in the massive and myriad programs of the Department. To identify potential problems in the programs, my staff has designed a number of computer applications. The computer applications, operated within the strictures of the Privacy Act and the computer match guidelines established by the Office of Management and Budget, are tailored to quantify specific identified vulnerabilities.

Some of our more successful computer applications, designed to combat health provider fraud and abuse, were published in July 1982.

Our second volume, published in September 1982, summarized computer applications designed to highlight illogical entitlement and invalid eligibility situations in the income maintenance and assistance programs.

This, our third volume, summarizes 25 computer applications designed to identify potential fraud and abuse in other Federal and State programs.

Although these computer applications were tailored to meet specific objectives, they may be applied to many diverse, but related, situations. In fact, we believe the extent to which they are adaptable is limited only by the imagination of the user.

Maximum benefits from the results of these applications can only be accomplished by sharing with those tasked with similar responsibilities at the Federal, State and local levels of Government.

By working together and sharing our successes, we can make government at all levels more cost effective and insure that vitally-needed funds reach only those recipients for whom they were intended.

October 1982

Richard P. Kusserow
Inspector General
Department of Health and
Human Services

COMPUTER APPLICATIONS

VOLUME III

PREFACE

The Inspector General of the Department of Health and Human Services is responsible for making more efficient an organization that is the largest distributor of funds in the Federal Government and whose annual budget is surpassed only by those of the United States and the Soviet Union. HHS spends over $250 billion annually on a variety of benefit, health service and research programs, ranging from Social Security, Medicare, Medicaid and Aid to Families with Dependent Children to the various health care and research programs of the Public Health Service.

Unfortunately, many of these vital programs are vulnerable to fraud, waste and abuse. The computer, therefore, has become a most important weapon in the crusade to make government more efficient and cost-effective.

Computer applications are an efficient and accurate means to review voluminous amounts of data. Further, the results provide a major starting point in the detection and prevention of fraud, waste and abuse in expensive government programs.

The Office of Inspector General has made substantial investments to recruit and develop the expertise to effectively and innovatively utilize computer technology. A unique computerized information retrieval system (HEWCAS), classroom exposure to EDP theory at our National Professional Development Center in Atlanta, and regional audit offices manned by a staff with advanced EDP training provide the resources to develop innovative computer applications.

Some of these are summarized in this compendium. Additional information on these computer applications can be obtained by contacting the National Professional Development Center, 1365 Peachtree Street, NE., Suite 400, Atlanta, Georgia 30309, (404) 881-2891.

VOLUME III

FEDERAL AND STATE PROGRAMS
FRAUD AND ABUSE

INVENTORY OF COMPUTER APPLICATIONS

PUBLIC ASSISTANCE ADMINISTRATIVE COSTS

III-1 To identify instances where the cost of equipment was charged as a direct expense to the program, but should have been included in the administrative cost pool.

III-2 To reconcile two sets of administrative cost accounting records.

STUDENT LOANS AND GRANTS

III-3 To identify situations where false information was used in applying for student-aid funds.

III-4 To identify instances where all economic resources were not considered in the student loan application process.

III-5 To identify inaccurate information in the data base which would result in the incorrect allocation of program funds.

III-6 To identify Department employees who are delinquent in student-aid loan repayments.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

III-7 To identify instances where time and effort charges were allocated to Federally sponsored research projects and training awards based on budgeted amounts rather than actual amounts.

III-8 To identify instances where teaching effort and related personal service costs were incorrectly charged to Federally sponsored research projects.

III-9 To identify instances where Federally sponsored research projects were charged for materials, equipment and supplies ordered near or after the completion date of the projects.

III-10 To identify the research efforts of principal investigators involved in Federally sponsored research projects.

III-11 To identify all cost transfers to Federally sponsored research projects not made within 120 days of the initial entry.

III-12 To identify by cost category the amount of direct costs charged to individual Federally sponsored research projects.

III-13 To identify the amount of unallowable indirect costs charged to Federally sponsored research projects.

III-14 To randomly select individuals whose effort was charged to Federally sponsored research projects.

III-15 To identify salary payments in excess of the base monthly rate charged to Federally sponsored research projects.

III-16 To identify, by class of employee, the salary costs charged to specific Federally sponsored research projects.

RETIREMENT, SURVIVORS AND DISABILITY INSURANCE PROGRAM--TITLE II OF THE SOCIAL SECURITY ACT

III-17 To determine whether earnings of State employees eligible for social security coverage were properly reported.

III-18 To determine whether FICA taxes were collected and paid on incidental compensation earned by covered employees.

III-19 To determine whether FICA taxes were collected and paid on earnings by exempt employees.

III-20 To determine whether the Treasury Department processed direct deposit transactions for social security payments to ineligible individuals.

III-21 To determine whether cashed social security payment checks from the Treasury Department or Social Security Administration were issued to individuals not recorded on the SSA Master Beneficiary record.

LOW INCOME ENERGY ASSISTANCE PROGRAM

III-22 To quantify overpayments made for the low income energy assistance program.

III-23 To identify improper energy assistance program payments made to public assistance recipients.

FEDERAL MEDICAL PROGRAMS

III-24 To identify duplicate payments to medical providers under Cuban Refugee program.

III-25 To determine whether medical services were claimed and paid after the recipients were no longer eligible.

PUBLIC ASSISTANCE ADMINISTRATIVE COSTS

Identified Vulnerability

The cost of equipment used in the administration of public assistance programs is an allowable cost. Equipment purchased specifically for use in a public assistance program is charged directly to the program. On the other hand, equipment purchased for use in a support or indirect function should be charged as an indirect cost. Accordingly, equipment costs are not expensed or charged off in the year of acquisition but are depreciated at a pre-established rate. Equipment purchased for use in an indirect function and charged as a direct cost to the public assistance program would result in an overcharge to the program.

OIG Action

A computer application was developed to identify and compute the unallowable charges in situations where equipment was purchased for use in an indirect function but was charged directly to the public assistance program.

Results

The program was successfully run in one location. A total of $1.7 million was identified as unallowable charges.

PUBLIC ASSISTANCE ADMINISTRATIVE COSTS

Identified Vulnerability

The State's official accounting records for public assistance programs are maintained by the designated fiscal department (State Department of Finance.) The records are a double entry accounting system.

The State agency also maintains its own single entry accounting system. The single entry system is the source of information for official financial reports.

To insure the financial integrity of the public assistance programs and the accuracy of claimed costs for administering the program, it is essential that two sets of accounting records be reconciled.

OIG Action

A computer application was developed to reconcile the financial information on the two sets of accounting records.

Results

The application was successfully run at one location. The financial information did not reconcile. Specific recommendations were made for correcting the identified problems.

STUDENT LOANS AND GRANTS

Identified Vulnerability

Information gathered during the grant application process is the basis for determining eligibility for educational student-aid programs. Misleading or erroneous information included in the application can result in an incorrect decision regarding eligibility. A combination of ineligibility and inaccurate reporting of educational accomplishments result in improper expenditures of Federal funds.

OIG Action

A series of computer applications were developed to isolate activities outside the norms established for applicants, students and institutions participating in the student-aid programs.

Results

The applications were tested during development. Results of the tests showed (1) individuals created numerous aliases to receive multiple payments of loans and grants, (2) institutions claimed enrollment and received funds for students who never attended the institutions or for students who were not attending during the period when funds were claimed, and (3) institutions incorrectly reported enrollment cancellations and computation of refunds.

The results of the tests were referred to investigative authorities.

STUDENT LOANS AND GRANTS

Identified Vulnerability

The Basic Economic Opportunity Grant program is designed to provide aid to low income students. In determining eligibility, it is necessary to consider all economic resources, including Social Security benefits.

OIG Action

A computer application was developed to compare information on the grant applications and information on Social Security Master Beneficiary Records.

Results

The program was run nationwide. A total of 113,340 grant applications did not reflect Social Security payments as an economic resource.

STUDENT LOANS AND GRANTS

Identified Vulnerability

The Migrant Student Record Transfer Systems (MSRTS) is a data base information system used in computing and allocating program funds. Inaccurate information in the data base would adversely impact the program.

OIG Action

A series of computerized screens based on Federal program requirements were developed. The screens were run against the data in the MSRTS.

Results

The application identified 1,006,000 entries of data which failed one or more of the screens. The results were referred to the Department of Education.

STUDENT LOANS AND GRANTS

Identified Vulnerability

Timely repayment of student loans by the borrowers provides a source of funds for future loans. Collection of delinquencies is, therefore, an important aspect of program administration. The Department's emphasis on collection included an in-house review.

OIG Action

Data from 37 schools was screened to identify delinquent borrowers. A computer application was developed to compare this information with HHS Payroll records.

Results

Eighty HHS employees with delinquent loans amounting to $68,000 were identified. Appropriate action is being taken.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Institutions develop budget estimates for the percentage of staff time which will be spent on various Federally sponsored research projects and training awards. Actual time and effort should be recorded during the project and budgeted amounts adjusted accordingly. If an employee has few changes in their time and effort distribution during the year, the practice of charging budgeted amounts may be occurring.

OIG Action

The OIG developed a computer application to identify the number of times employees of the institution changed their time and effort distributions.

Results

The application was successfully run at one location.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

University faculty who work on Federally sponsored research projects may also be involved in teaching activities. The teaching effort and the related personal services costs are unallowable charges to the research projects because teaching activities primarily benefit a university instructional program rather than the research program.

OIG Action

A computer application was developed to identify the total costs of teaching activities charged to Federally sponsored research projects.

Results

The application was successfully run at one location. Unallowable teaching salaries, related fringe benefits and indirect costs totaling $408,000 were identified.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Material, supplies and equipment for Federally sponsored research projects are ordered and received during the period of project performance. Controls are necessary, however, to ensure delivery dates are within the period where the items are needed in the project. Although orders may be placed early during the performance period, controls should be established to monitor delivery dates to ensure cancellation if delivery dates are too late to benefit the project.

OIG Action

A computer application was developed to select a sample of material, supplies, and equipment received near the end or after the completion of the project.

Results

The application was successfully run at two locations. Purchases of material, supplies and equipment totaling $250,000 were identified for review.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerabillity

For some research projects the amount of Federal support is directly related to the amount of funding for relevant non-Federal research projects. Therefore, it is important for the institution to accurately record and properly allocate the amount of cost-sharing for the non-Federal research projects.

OIG Action

A computer application was developed to list project funding for all Federal and non-Federal research projects associated with individuals acting as principal investigators.

Results

The application was successfully run at one location.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Research institutions having Federally sponsored research projects sometimes transfer costs between projects. It is, therefore, important to have procedures to insure the accuracy and appropriateness of cost allocation between projects.

OIG Action

A computer application was developed to identify cost transfers not made within 120 days of the initial entry.

Results

The application was successfully run at one location. Unallowable costs totaling $1.5 million were identified.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Research institutions involved in Federally sponsored research projects generate large amounts of costs charged directly to the projects. Determining the propriety of these direct costs requires an extensive review effort. The task can be simplified if the costs by project and the individual elements within each project are known before beginning the review.

OIG Action

A computer application was developed to list the total costs by category within each Federally sponsored research grant or contract. Further, the applications categorized the research projects by awarding Federal agency.

Results

The application was run successfully at one location.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Indirect costs are recognized as an allowable claim of Federally sponsored research funds. The percent of indirect costs that are allowable is negotiated between the university and the Federal Government. Sometimes, several rates are negotiated with a university. Therefore, it is important to establish controls to insure the proper negotiated rate is used in computing indirect cost allocations.

OIG Action

A computer application was developed to calculate the allowable indirect costs for each Federal project, compare the amount calculated with the amount of indirect costs charged and compute any overclaims.

Results

The application was run successfully at one location. Unallowable indirect costs totaling $118,000 were identified.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Salaries and related personal services costs represent the largest amount of costs charged to Federally sponsored research projects. It is important, therefore, that officials who certify the effort devoted to a project are aware of what activites individual researchers are actually engaged in so effort can be properly distributed to the individual projects.

OIG Action

A computer application was developed to randomly select individuals devoting effort to on-going projects.

Results

The application was successfully run at one location. Results are being reviewed.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

University faculty salaries are established by the university's compensation plan. Even when the salaries earned are greater than the base monthly rate, only the base monthly rate can be charged to Federally sponsored research projects.

OIG Action

A computer application was developed to identify those salaries charged in excess of the base monthly rate to compute the excess claimed.

Results

The application was run successfully at one location. Unallowable salaries and related personal services costs of $160,000 were identified.

COLLEGES, UNIVERSITIES AND OTHER NONPROFIT ORGANIZATIONS

Identified Vulnerability

Major research institutions have many Federally sponsored research projects in process at all times. Within any given time period, there may be different classes of employees working on projects. Therefore, certification by class of employees is essential for accurate cost allocation to the various projects.

OIG Action

A computer application was developed to summarize payroll charges, by class of employee, to Federally sponsored research projects.

Results

The application was successfully run at one location.

RETIREMENT, SURVIVORS AND DISABILITY INSURANCE PROGRAM--TITLE II OF THE SOCIAL SECURITY ACT

Identified Vulnerability

Section 218 of the Social Security Act established eligibility of certain State employees for Social Security coverage. It is especially important for eligible State employees' earnings to be reported for the first quarter of membership.

OIG Action

A computer application was developed to compare State retirement system history records with the Social Security Summary Earnings Record to identify unreported earnings.

Results

The program was successfully run for two locations. No problems were identified.

RETIREMENT, SURVIVORS AND DISABILITY INSURANCE PROGRAM-- TITLE II OF THE SOCIAL SECURITY ACT

Identified Vulnerability

The law requires FICA taxes to be withheld from incidental compensation paid to covered employees. Payroll systems may not have procedures for deducting and reporting the FICA taxes from incidental compensation.

OIG Action

A computer application was developed to identify covered employees receiving incidental compensation. The application listed all employees receiving incidental compensation where the maximum FICA taxes had not been withheld.

Results

The program was successfully run at one location. The results are being reviewed.

RETIREMENT, SURVIVORS AND DISABILITY INSURANCE PROGRAM--TITLE II OF THE SOCIAL SECURITY ACT

Identified Vulnerability

Earnings of employees participating in certain retirement programs are exempt from Social Security coverage. Some payroll systems may not have procedures to identify the exempt employees.

OIG Action

A computer application was developed to identify exempt employees whose earnings were reported as covered by Social Security.

Results

The application was successfully run at one location. No problems were identified.

RETIREMENT, SURVIVORS AND DISABILITY INSURANCE PROGRAM--TITLE II OF THE SOCIAL SECURITY ACT

Identified Vulnerability

The Treasury Department processes direct deposit transactions for Social Security payments. Information developed from other audits indicated the Treasury Department could make direct deposit payments for individuals who were not eligible to receive Social Security benefits.

OIG Action

A computer application was developed to compare a sample of Treasury Department payment data with the SSA's Master Beneficiary Records to identify any payments to ineligible beneficiaries.

Results

The application was run nationwide. No problems were identified.

RETIREMENT, SURVIVORS AND DISABILITY INSURANCE PROGRAM--TITLE II OF THE SOCIAL SECURITY ACT

Identified Vulnerability

Checks for Social Security benefits can be prepared manually by the Social Security Administration or the Treasury Department, without the payments being recorded on the Master Beneficiary Record.

OIG Action

A sample of cashed checks were selected. A computer application was developed to compare the Master Beneficiary Record with the information on the cashed checks.

Results

The application was successfully run at SSA. No problems were identified.

LOW INCOME ENERGY ASSISTANCE PROGRAM

Identified Vulnerability

The Low Income Energy Assistance Program payments were computed according to a State plan. The State plan stipulated the amount (ceiling) each household could receive. Payments were made based on this ceiling. Subsequently, the State plan was revised and the ceiling was increased. This change necessitated a second payment. Override procedures were made in the payment system to process a second payment. Since override procedures were necessary, additional edits should have been developed to preclude payments exceeding the higher established ceiling.

OIG Action

A computer application was developed to identify all payments exceeding the revised ceiling.

Results

The application was successfully run at one location. Approximately $394,000 in overpayments were identified.

LOW INCOME ENERGY ASSISTANCE PROGRAM

Identified Vulnerability

To be eligible for benefits under the Low Income Energy Assistance Program, a recipient must have received a public assistance grant or general assistance program grant for or during a specific time period.

OIG Action

A computer application was developed to identify ineligible recipients. Additionally, the application computed correct benefits for eligible recipients and compared this amount with recorded payments.

Results

The application was successfully run in one location. Overpayments of $53,000 to 449 recipients were identified.

FEDERAL MEDICAL PROGRAMS

Identified Vulnerability

Under the Cuban Refugee Program, payments are made to providers of medical services for refugees. Medical providers could file claims for the same service under more than one identification number or more than one provider could bill for the same service. Duplicate billings would result if controls in the payment system did not identify these billing practices.

OIG Action

A computer application was developed to list all instances where more than one claim was paid for the same medical service on the same date for the same individual.

Results

The program was run nationwide. Over $250,000 in duplicate payments were identified.

FEDERAL MEDICAL PROGRAMS

Identified Vulnerability

Under the Cuban/Haitian Refugee Program, the Public Health Service paid for medical services while the refugees were in the custody of U.S. officials. After release from custody, the refugees were no longer eligible for payment of medical services by the PHS. If edits were not in place to compare the date of medical services with the date of release from custody, overpayments could result.

OIG Action

A computer application was developed to identify claims for medical services provided after the date refugees had been removed from custody roles.

Results

The program was successfully run nationwide. Five thousand, six hundred claims totaling $1.6 million were processed for services provided to 2,800 refugees after the dates they were released from custody. Further review is in process.

PROJECT SONOMA

In late 1980, the Office of Investigations, Sacramento, initiated Project Sonoma in an effort to identify "welfare queens" who were fraudulently collecting large payments through the county welfare system. Based upon experiences in other investigations and projects, our investigators, working with the California State Fraud Prevention Bureau and the County of Sonoma, isolated certain factors common to this type of fraud.

General relief cases were screened out for all cases where there were no children under the age of six (6); where there was either earned or unearned income and where there was a case consisting of a mother and an unborn. The resultant purified file was then matched against the SSA numadent.

The Sonoma County welfare roll of 6,000 cases was run against a profile of these factors, and after a name and social security validation process, 74 cases of potential fraud were identified.

Because of limited manpower and resources, the OI investigative unit was able to complete only eight investigations before being required to reduce its involvement for other priorities.

The results of those eight cases were as follows:

A. Three cases the recipient possessed a valid social security card with the questioned numbers, copies of cards and/or originals forwarded to Tom Sheehan.

B. One case of apparent honest error--transposition of numbers by recipient. No fraud.

C. One case of recipient error transposition, no welfare fraud uncovered--however, is probably related to forgery scheme in private sector. Appropriate referral made.

D. One case(s) we have not uncovered any substantiated fraud, however; due to the fact the former recipient's case is closed and whereabouts unknown, we were unable to physically examine their social security cards to verify the numbers.

E. One case the recipient failed to cooperate--walking out of the interview--unable to verify social security number. This aid case was discontinued--current whereabouts unknown. From all review procedures this case appears to be legitimate, however, recipient may have had a boyfriend residing in the home.

F. One case revealed that the recipient was employed under her correct social security number--not reporting the income and was residing with the employed father of her aided children. This investigation resulted in a criminal complaint still pending in court alleging a total of overpayments at $4,333.00.

WILLIAM V. ROTH, JR., DEL., CHAIRMAN

CHARLES H. PERCY, ILL.
TED STEVENS, ALASKA
CHARLES MC C. MATHIAS, JR., MD.
JOHN C. DANFORTH, MO.
WILLIAM S. COHEN, MAINE
DAVID DURENBERGER, MINN.
MACK MATTINGLY, GA.
WARREN B. RUDMAN, N.H.

THOMAS F. EAGLETON, MO.
HENRY M. JACKSON, WASH.
LAWTON CHILES, FLA.
SAM NUNN, GA.
JOHN GLENN, OHIO
JIM SASSER, TENN.
DAVID PRYOR, ARK.
CARL LEVIN, MICH.

JOAN M. MC ENTEE, STAFF DIRECTOR

SUBCOMMITTEE:
WILLIAM S. COHEN, MAINE, CHAIRMAN

TED STEVENS, ALASKA
WARREN B. RUDMAN, N.H.

CARL LEVIN, MICH.
DAVID PRYOR, ARK.

SUSAN M. COLLINS, STAFF DIRECTOR

United States Senate
COMMITTEE ON
GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON
OVERSIGHT OF GOVERNMENT MANAGEMENT
WASHINGTON, D.C. 20510

August 27, 1982

The Honorable Richard S. Schweiker
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Schweiker:

On September 23, the Subcommittee on Oversight of Government Management will hold a hearing on the use of computer matching to detect fraud or waste in government programs. To assist the Subcommittee in preparing for this hearing, I request that the appropriate HHS official(s) provide me with information about "Project Match," which was conducted by the Office of the Inspector General in the Department of Health, Education and Welfare in 1976, and about "Operation Cross Check," in which the HEW matched delinquent student loan records with lists of federal workers.

In addition to a general description of each project, please provide responses to the following questions:

(1) What was the legal authority for conducting the matches?

(2) What were the goals of the matches?

(3) What procedures were used in conducting the matches; for example, which computer tapes were matched?

(4) Please provide the beginning and ending dates for each project.

(5) Which federal agencies exchanged computer tapes or other information to permit the match to be conducted?

(6) Were any requests made to private businesses or to state agencies for information or computer lists to be used in the projects? If so, please describe these requests and indicate the computer tapes or other information that was supplied by private businesses or state agencies.

(7) How many "raw hits" were obtained from the matches conducted under the projects?

(8) How many "raw hits" obtained from the matches were investigated?

(9) How many "raw hits" resulted in prosecution; how many cases were dismissed or dropped prior to prosecution; how many were successfully prosecuted?

(10) How much money did the federal government actually recover as a result of cases uncovered through the projects? What was the average amount of recovery per individual investigated?

(11) What was the final cost of the projects? Please break down the cost figures into specific factors, for example, computer time, investigative costs, staff hours expended, prosecution costs.

(12) Were cost-benefit analyses performed prior to conducting the matches?

(13) Were reports of the projects published in the Federal Register, provided to Congress, or released to the public? If so, please provide me with a copy of such reports.

(14) Why were the projects ended?

In order to provide the Subcommittee adequate time to review your response, please supply this information to the Subcommittee on or before September 10. Please have the response delivered to the Subcommittee office at 506 Carroll Arms, 301 1st Street, N.E.

The Honorable Richard S. Schweiker
Secretary
Department of Health and Human Services
August 27, 1982
Page 3

Thank you for assisting the Subcommittee in evaluating computer matching. If you have any questions, please have your staff contact Mary Gerwin or Susan Collins of the Subcommittee staff, at 224-5538.

With best wishes, I am

Sincerely,

William S. Cohen
Chairman

WSC:mbg

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

SEP 10 1982

The Honorable William S. Cohen
United States Senate
Chairman, Subcommittee on Oversight
 of Government Management
506 Carroll Arms
301 1st Street, N.E.
Washington, D.C. 20510

Dear Senator Cohen:

Secretary Schweiker has asked me to respond to your letter of August 27. I appreciate the opportunity to assist the Subcommittee in preparing for its hearing on the use of computer matches to detect fraud and waste in Government programs. The elimination of fraudulent and wasteful expenditures is a goal I share with you.

As requested, a general description and responses to specific questions relating to "Project Match" and "Operation Cross Check" are included as Enclosures I and II respectively. The responses follow the sequence of the questions.

Project Match was designed to join the Office of Inspector General (OIG) and the States in a common effort to eliminate fraud and abuse in the Aid to Families with Dependent Children (AFDC) program. The OIG role was to match State AFDC rolls with Federal employee rolls to identify raw hits. Raw hit data was provided to the various States to verify validity and, where warranted, take necessary prosecutory action. Accordingly, information relative to prosecutions, convictions, collections and cost was generated by multiple sources. As the States were not required to furnish us such data, overall statistics were not developed. We were, however, able to obtain conviction data from 44 States by means of telephone solicitation.

Cross Check was designed to identify Federal employees who were in default on loans obtained through the Guaranteed Student Loan Program (GSLP). The OIG matched Federal employee (civilian and military) rolls with Office of Education (OE) default records and identified raw hits. A listing of raw hits was turned over to the Office of Education (now the Department of Education). HHS has no further responsibility for the project.

We will be pleased to furnish you any additional information you may require.

Sincerely yours,

Richard P. Kusserow
Inspector General

Enclosures

PROJECT MATCH

General Description

The OIG, HHS initiated Project Match in 1977 with the objective of reducing fraud and abuse in the Aid to Families with Dependent Children (AFDC) program. The project was designed to identify Federal employees who were illegally receiving AFDC benefits and to provide a basis for corrective actions.

Basically, the project matched States' AFDC rolls with Federal civilian active and retired employee and active duty military personnel rolls provided by the Office of Personnel Management (OPM) and the Department of Defense (DOD). The rolls were compared by computer to identify cases where individuals appeared on both rolls (raw hits). Raw hits were not necessarily indicative of impropriety. They were forwarded to State welfare agencies to verify employment and determine AFDC eligibility.

Specific Information

(1) Project Match was conducted as part of the OIG's responsibility, under 42 U.S.C. 3523(a), to supervise, coordinate, and provide policy direction with respect to investigations and other activities designed to prevent and detect fraud and abuse in programs administered or financed by HHS. Under 42 U.S.C. 3525(a), the OIG is authorized access to all records which relate to programs and operations over which the OIG has responsibility. This section also authorizes the OIG to request information or assistance from any Federal, State, or local Government agency when necessary to carry out its duties and responsibilities.

Specific statutory authority is not required to conduct computer matches. However, various confidentiality statutes such as the Privacy Act of 1974, 5 U.S.C. 552a, must be complied with in order to collect, maintain, and release certain classes of records. Project Match was performed in conformance with the Privacy Act. Current matching projects must also comply with the Office of Management and Budget's (OMB) Revised Supplemental Guidance for Conducting Computerized Matching Programs, 47 Fed. Reg. 21656 (May 19, 1982), which replaced earlier OMB guidance on computer matchings issued on March 30, 1979. Project Match pre-dated these guidelines.

(2) The project was part of a continuing program to reduce and prevent fraud and abuse in HHS programs. It was a Federal/State effort to identify Federal employees who may be improperly receiving AFDC assistance. These cases were referred to States for appropriate criminal or administrative action.

(3) HHS obtained from OPM, pursuant to a Memorandum of Understanding dated August 18, 1977, a computer tape containing the name, grade, salary, date of birth, Social Security Number, employing agency, and work location of some 2.8 million Federal civilian employees and about 600,000 retired or separated civilian employees. DOD, pursuant to a Memorandum of Understanding and a routine use published in the Federal Register on January 18, 1978, provided HHS with payroll tapes containing similar data for about 1.5 million active duty military personnel in the United States. These tapes were matched with State AFDC recipient tapes.

(4) During the Spring of 1977, we reviewed cooperative efforts by U.S Attorneys, Postal Service, Internal Revenue and State officials to identify welfare cheaters on the Federal payroll in Detroit, Michigan, and Chicago, Illinois. Based on their observations of apparent fraud, in 1977 a pilot test by HHS-OIG was made in the District of Columbia by matching the District's AFDC rolls against the HHS payroll. This was the starting point for Project Match.

(5) OPM and DOD provided computer tape data to HHS.

(6) Initially, 26 jurisdictions (24 States, the District of Columbia and New York City) submitted AFDC computer data. This included the State code; recipient's name, address, date of birth, and Social Security Number; and beginning eligibility date for AFDC payment. Other States were asked to participate in March 1978. A total of 52 jurisdictions contributed data. No businesses were asked for or contributed information.

(7-11) There were 33,000 raw hits. After eliminating cases with low earnings, and individuals no longer employed, the number warranting follow-up for determination of eligibility was reduced to 19,713.

Of the 19,713 cases, about 29 percent were determined to be overpaid or ineligible. As the States were not required to inform HHS on the number of prosecutions, convictions, etc., complete data is not readily available. However, some data was obtained by telephone interview with States (See Exhibit A).

(12) Since this was a new and innovative approach, specific cost benefit analyses were not performed. Also, prior to publication of OMB matching guidelines in March 1979, there was no requirement for cost-benefit analyses. Such reviews should be a major deterrent to fraudulent AFDC claims. However, the impact of the deterrence factor cannot be readily measured.

(13) Reports were published in the Federal Register; data on the project was included in the Inspector General Annual Report to the Congress for 1978 and 1979; and several news releases and statements were made. Copies are attached.

(14) The OIG has instituted measures to update the match by publishing both a system of records and a matching report in the Federal Register to comply with the Privacy Act and OMB's guidance for matching programs.

EXHIBIT A

AFDC CONVICTIONS BY STATE 1978[1]

State	Number of Convictions
Region I	
Connecticut	368[2]
Maine	1
Massachusetts	28
New Hampshire	15
Rhode Island	79
Vermont	38
Region II	
New Jersey	381
New York	1,700 (Est.)
Region III	
Delaware	5 (Est.)
District of Columbia	69
Maryland	138
Pennsylvania	369
Virginia	364[3]
West Virginia	4
Region IV	
Alabama	100
Florida	1,076
Georgia	282
Kentucky	247
Mississippi	11
Tennessee	25
Region V	
Illinois	181
Indiana	57
Michigan	322[4] (Est.)
Minnesota	165
Wisconsin	181
Region VI	
Arkansas	25
Louisiana	79
New Mexico	38[5] (Est.)
Oklahoma	12
Texas	358
Region VII	
Iowa	36
Kansas	115 (Est.)
Missouri	101
Region VIII	
Colorado	7
Montana	57
North Dakota	10
South Dakota	49[5]
Utah	48
Region IX	
Arizona	21 (Est.)
California	2,639
Region X	
Alaska	2
Idaho	2
Oregon	142
Washington	477
TOTAL	10,424 (Est.)

1/ State Fiscal Year may be other than October to September
2/ The majority of this figure represents AFDC convictions
3/ This figure is the accumulated total over a 9 month period
4/ Number represents estimate of 35 counties
5/ Number represents estimate over 14 month period

The figures on the number of AFDC convictions represent responses given in a telephone interview with each of the respective States. It should be noted that these figures include estimates from State officials who have taken on-the-spot polls in an effort to determine the conviction numbers. There appears to be a problem in ascertaining the number of AFDC convictions in several States due to the lack of a centralized data collection unit and/or fraud unit which tracks this type of information.

Source: HHS Inspector General Annual Report--1978

Enclosure II

OPERATION CROSS CHECK

General Description

Cross Check was designed to identify Federal employees, civilian and active duty military, who appeared to be in default on loans obtained through the Guaranteed Student Loan Program (GSLP) and where appropriate, to take action to accelerate recoveries on defaulted loans. Cross Check was implemented in three phases: Phase I was a pilot project conducted in the Fall of 1977 using HHS' own payroll; Phase II initiated in February 1978, included the entire Federal active civilian work force; and Phase III initiated in November 1978 included the Federal active military employee data base. In each phase, the default file of the Office of Education was compared, by computer, with a file of Federal employees to identify possible loan defaulters.

OE attempted routine collection efforts prior to seeking collection assistance from the employing agency. Where this was not successful, OE requested the employing agency to counsel the employee on the need for repayment. Accounts which remained unresolved after a counseling effort were reviewed and referred where appropriate for litigation.

Specific Information

(1) Cross Check was conducted as part of the OIG's responsibility, under 42 U.S.C. 3523(a), to supervise, coordinate, and provide policy direction with respect to investigations and other activities designed to prevent and detect fraud and abuse in programs administered or financed by HHS. Under 42 U.S.C. 3525(a), the OIG is authorized access to all Department records which relate to programs and operations over which the OIG has responsibility. This section also authorizes the OIG to request information or assistance from any Federal, State, or local Government agency when necessary to carry out its duties and responsibilities.

Specific statutory authority is not required to conduct computer matches. However, various confidentiality statutes such as the Privacy Act of 1974 must be complied with in order to collect, maintain, and release certain classes of records. Cross Check was performed in conformance with the Privacy Act. Current matching projects must comply with the OMB's Revised Supplemental Guidance for Conducting Computerized Matching Programs, 47 Fed. Reg. 21656 (May 19, 1982), which replaced earlier OMB guidance on computer matchings issued on March 30, 1979. Cross Check pre-dated these guidelines.

(2) Cross Check was launched as part of HHS' comprehensive program to locate all GSLP defaulters, and to accelerate recoveries on defaulted accounts.

(3) By Memorandum of Understanding dated August 18, 1977 between the OPM and HHS, OPM provided a computer tape which included such items as name, grade, salary, date of birth, Social Security Number, employing agency and work location for 2.8 million Federal civilian workers and about 600,000 retired or separated civilian employees. Later, similar data was received from DOD for 1.5 million active duty military personnel.

(4) Cross Check started in the fall of 1977 and presently is the responsibility of the Department of Education.

(5) OPM and DOD provided HHS with computer tapes.

(6) No tapes were requested from States or private business firms.

(7-9) Phase I identified 317 HHS employees in default. Of this number 101 no longer worked for the Department. Of the remaining 216, 168 were resolved and 48 were referred for litigation. Phase II identified 6,600 other civilian employees in default. Exhibit B shows progress in resolving these accounts. Phase III identified 9,930 military employees in default. HHS has no data on resolutions. Data may be available from the Department of Education which now has overall responsibility for the GSLP.

(10) Data on amounts recovered are not readily available. Potential recoveries for Phase I were estimated to be between $250,000 and $300,000. Phase II and III involved defaults of about $15.8 million. Data may be available from the Department of Education.

(11-12) No records are available on specific cost factors or total costs of the project. Since this was a new and innovative approach, cost-benefit analyses were not performed prior to initiating the matches. Also, prior to publication of OMB matching guidelines in March 1979, there was no requirement for cost-benefit analyses. However, two benefits surfaced: (1) students began repaying defaulted loans, and (2) the visibility of the project should encourage students to repay, rather than default on their loans.

(13) Reports were published in the Federal Register; data on the project was included in the Inspector General Annual Reports to the Congress for 1978 and 1979; and various news releases and statements were made. Copies are attached.

(14) As noted (7-9), Phase I (HHS employees) and Phase II (civilian work force) were completed. Phase III was turned over to the Department of Education which has responsibility for the GSLP.

WILLIAM V. ROTH, JR., DEL., CHAIRMAN
CHARLES H. PERCY, ILL.
TED STEVENS, ALASKA
CHARLES MC C. MATHIAS JR., MD.
JOHN C. DANFORTH, MO.
WILLIAM S. COHEN, MAINE
DAVE DURENBERGER, MINN.
MACK MATTINGLY, GA.
WARREN B. RUDMAN, N.H.

THOMAS F. EAGLETON, MO.
HENRY M. JACKSON, WASH.
LAWTON CHILES, FLA.
SAM NUNN, GA.
JOHN GLENN, OHIO
JIM SASSER, TENN.
DAVID PRYOR, ARK.
CARL LEVIN, MICH.

JOAN M. MC ENTEE, STAFF DIRECTOR

WILLIAM S. COHEN, MAINE, CHAIRMAN
TED STEVENS, ALASKA
WARREN B. RUDMAN, N.H.

SUSAN M. COLLINS, STAFF DIRECTOR

United States Senate
COMMITTEE ON
GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON
OVERSIGHT OF GOVERNMENT MANAGEMENT
WASHINGTON, D.C. 20510

October 4, 1982

The Honorable Terrel H. Bell
Secretary
Department of Education
400 Maryland Avenue, N.W.
Washington, D.C. 20202

Dear Mr. Secretary:

The Senate Subcommittee on Oversight of Government Management is examining the use of computer matching to detect fraud and waste in government agencies. To assist the Subcommittee in preparing for its hearings, I request that the appropriate Department of Education official(s) provide me with the following information about "Operation Cross Check" that was conducted by the Department of Health, Education and Welfare in 1977 and 1978, and about other matches that the Department of Education has or is now conducting.

(1) How many "raw hits" that were identified in Phases II and III of "Operation Cross Check" were investigated?

(2) How many "raw hits" identified in Phases II and III resulted in prosecution? How many cases were dropped or dismissed prior to prosecution? How many were successfully prosecuted?

(3) How much money did the federal government actually recover as a result of the cases uncovered during Phases II and III of "Operation Cross Check?"

(4) What was the final cost to the Department of Education of "Operation Cross Check?" Please break down the cost figure into specific factors; for example, computer time, investigative costs, staff hours expended, prosecution costs.

(5) Were cost-benefit analyses performed prior to conducting the matches in Phases II and III of "Operation Cross Check?"

(6) Why was "Operation Cross Check" ended?

(7) Has the Department of Education conducted other matching projects involving other federal government agencies since 1978? If yes, please provide the following information concerning each project:

   (a) a general description of the matching project and the purpose for conducting the match;

   (b) the federal agencies that cooperated in the match by giving computer lists to the Department of Education and a copy of any inter-agency agreements governing the match;

   (c) the number of "raw hits" that were obtained in each project;

   (d) the number of "raw hits" that have been or are being investigated or prosecuted;

   (e) the amount of money that the Department of Education actually recovered as a result of uncovering cases through the project;

   (f) the final cost of each project. Please break down the cost into specific factors, such as those listed in question #4.

   (g) Were any cost-benefit analyses performed prior to conducting the match?

   (h) Were reports of the project published in the Federal Register provided to Congress, or released to the public? If so, please provide me with a copy of such reports.

   (i) Has the Department of Education recommended that the project be repeated or conducted on a larger scale?

Please provide the Subcommittee with this information on or before October 20. Please have the response delivered to the Subcommittee office at 506 Carroll Arms, 301 1st Street, N.E., or mailed to the Subcommittee on Oversight of Government Management, Committee on Governmental Affairs, 3306 Dirksen Senate Office Building, Washington, D.C. 20510.

Your assistance is greatly appreciated. If you have any questions, please have your staff contact Mary Gerwin or Susan Collins of the Subcommittee staff at 224-5538.

With best wishes, I am

Sincerely,

William S. Cohen
Chairman

WSC:mbg

THE SECRETARY
WASHINGTON, D.C. 20202

OCT 21 1982

Honorable William S. Cohen
Chairman, Subcommittee on Oversight
of Government Management
Committee on Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Senator Cohen:

Enclosed is our response to the questions raised in your letter of October 4, 1982, regarding "Operation Cross Check" conducted by the Department of Health, Education, and Welfare (DHEW) in 1977 and 1978 and about other matches that the Department of Education has or is now conducting. Our response is presented in the order the questions were asked.

We are unable to provide complete information on the prior DHEW project as portions of the files could not be located.

The ED matching project is significantly larger than "Operation Cross Check". DHEW matched defaulted Federally Insured Student Loans (only part of the Guaranteed Student Loan Program) with Federal personnel files. The current ED matching project involves loans defaulted under the Guaranteed Student Loan Program and the National Direct Student Loan Program which constitutes a much larger universe.

Since only the initial phases of the current project have been completed, some of the detailed information you requested is not available.

Please advise us if you would like any further information on this matter. Thank you for your interest.

Sincerely,

T. H. Bell

Enclosures

Enclosure 1

The required information follows in a question/answer format referenced to your letter dated October 4, 1982. Only limited data relevant to "Operation Cross Check," conducted by the Department of Health, Education, and Welfare, is available to the Department of Education.

(1) How many "raw hits" that were identified in Phases II and III of "Operation Cross Check" were investigated?

According to available records most of the raw hits identified in Phases II and III of "Operation Cross Check" received investigative/administrative action. The table "Operation Cross Check" (Enclosure 2) shows the status of the project as of April, 1980.

(2) How many "raw hits" identified in Phases II and III resulted in prosecution"? How many cases were dropped or dismissed prior to prosecution? How many were successfully prosecuted?

As shown in Enclosure 2, a total of 1,994 cases were referred for follow up action by the U.S. Attorney. However, our records do not contain the results of the referrals.

(3) How much money did the federal government actually recover as a result of the cases uncovered during Phases II and III of "Operation Cross Check?"

Statistics on the amount of money actually recovered during "Operation Cross Check" are not available. During the implementation of the project, potential recoveries were estimated to approach 65-75% of the value of the outstanding loan accounts or from $12.7 to $14.7 million.

(4) What was the final cost to the Department of Education of "Operation Cross Check?" Please break down the cost figure into specific factors; for example, computer time, investigative costs, staff hours expended, prosecution costs.

The costs incurred for the actual computer matching of the records were estimated to be less than $2,000. The cost of follow up activities--collection, counseling, litigation--were considered activities normally conducted by HEW and other Federal agencies in the normal performance of their duties and responsibilities. Our files do not indicate that these costs were segregated.

(5) Were cost-benefit analyses performed prior to conducting the matches in Phases II and III of "Operation Cross Check?"

Available records indicate that cost-benefit analyses were performed prior to conducting the matches in Phases II and III of "Operation Cross Check". The actual computer matching of the records were estimated to be less than $1,000 for each phase. The follow-up activities--collection, counseling, litigation--were considered activities normally conducted by HEW and other Federal agencies in the normal performance of their duties and responsibilities. Our files do not indicate that these latter costs were separately considered.

(6) Why was "Operation Cross Check" ended?

"Operation Cross Check" was initiated by the Department of Health, Education, and Welfare to identify Federal employees in default on their Federally Insured Student Loans and to take appropriate action to accelerate recoveries on the defaulted loans. The total project was estimated to be completed by June 1979. However, we are unable to provide a precise reason as to why the project ended or when it actually did end.

(7) Has the Department of Education conducted other matching projects involving other Federal government agencies since 1978? If yes, please provide the following information concerning each project:

(a) a general description of the matching project and the purpose for conducting the match;

In August 1982 the Department of Education (ED) Office of Inspector General (OIG) initiated a one-time computer match of Federal personnel files with Education Department files on defaulted student loans. The specific objectives of the matching program are: (1) to locate Federal personnel (civilian, military, current and retired) in default on loans made under the Guaranteed Student Loan and National Direct Student Loan Programs; (2) to increase collection of defaults and reduce outstanding defaults of Federal employees by referring cases to their employing agencies for appropriate administrative action; and (3) to refer cases to United States Attorneys for enforced collection where appropriate.

(b) the federal agencies that cooperated in the match by giving computer lists to the Department of Education and a copy of any inter-agency agreements governing the match;

The Veterans Administration (VA) performed the actual match using VA computer equipment and personnel under the direction of the ED/OIG staff. ED's student loan default files were provided to VA which is responsible during the conduct of the match program for providing central storage, duplication, and control of the Federal personnel files involved in the match. The Department's defaulted loan records were matched against Federal personnel files from four Federal agencies (Office of Personnel Management, Department of Defense, Department of Transportation--U.S. Coast Guard, and the Tennessee Valley Authority).

The systems of records of the four Federal agencies which were used in the matching program follows:

1. The Office of Personnel Management:

a. OPM/CENTRAL-1, Civil Service Retirement and Insurance Records, and b. OPM/GOVT-1, General Personnel Records, published in the FEDERAL REGISTER on April 16, 1982 (47 FR 16474 and 16489).

2. The Department of Defense

S322.10 DLA-LZ Defense Manpower Data Center published in the FEDERAL REGISTER January 18, 1982 (47 FR 2751), April 15, 1982 (47 FR 16193) (New routine use amendment to systems of records).

3. The Department of Transportation-U.S. Coast Guard

a. U.S. Coast Guard 525, Active Duty Payroll System, and b. U.S. Coast Guard 624, Personnel Management Information System (PMIS), published in the FEDERAL REGISTER December 7, 1981 (46 FR 59752 and 59766).

4. The Tennessee Valley Authority:

a. TVA-2, Personnel Files, b. TVA-11, Payroll Records, and (c) TVA-26 Retirement System Records, published in the FEDERAL REGISTER February 12, 1980 (45 FR 9428, 9435, 9445), and December 29, 1981 (46 FR 62993) (New routine use amendment to system of records.)

(c) the number of "raw hits" that were obtained in each project;

(d) the number of "raw hits" that have been or are being investigated or prosecuted;

(e) the amount of money that the Department of Education actually recovered as a result of uncovering cases through the project;

(f) the final cost of each project. Please break down the cost into specific factors, such as those listed in question #4.

Since this project is not yet completed, answers to these four questions are not yet available.

(g) Were any cost-benefit analyses performed prior to conducting the match?

The financial costs and benefits of conducting a computer match were considered prior to the initiation of the matching program. The primary objective of the matching program is to identify Federal employees who are in default on their guaranteed loans and to bring these individuals, where appropriate, into repayment. Computer comparison of systems of records is the only cost effective method available to provide comprehensive identification of Federal employees in default on student loans. Further, most of the activities involved in the matching program--collection processing, counseling and litigation--are considered activities normally conducted by the Department and other Federal agencies in the normal performance of their duties and responsibilities. However we will attempt to capture the costs of these activities.

(h) Were reports of the project published in the Federal Register provided to Congress, or released to the Public" If so, please provide me a copy of such reports.

"Notice of Matching Programs" as required by the Office of Management and Budget's (OMB), Revised Supplemental Guidance for Conducting Matching Programs, of May 11, 1982, is being processed for publication in the Federal Register. A copy of this notice will be provided to both Houses of Congress and OMB when the notice is sent to the Federal Register for publication.

(i) Has the Department of Education recommended that the project be repeated or conducted on a larger scale?

The current matching program builds on the prior matches conducted by the Department of Health, Education, and Welfare. However, the current program is being conducted on a larger scale than that of DHEW. In 1977 and 1978, the computer matching program involved 300,000 defaulted Federally insured loans valued at approximately $300 million. The current matching program includes the National Direct Student Loan Program as well as the Guaranteed Student Loan programs for a total of over 800,000 defaulted loans valued at over $1 billion.

Enclosure 2

OPERATION CROSS CHECK
DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE

(As of April 1980)

	Phase II (Federal Civilian Employees)	Phase III (Federal Military Employees)	Total
Defaulters Identified	6,600	10,740	17,340
No Longer Employed	1,891	314	2,205
Entitled to Military Deferment	0	810	810
Paid in Full	689	674	1,363
In Repayment or Promised to Pay	2,960	3,442	6,402
Referred to Litigation	592	1,402	1,994
Compromised/Ceased Action	468	188	656
Unresolved (as of April 1980)	0	3,910	3,910
Estimated Value of Accounts at time of Match	$7.5 million	$12.1 million	$19.6 million

WILLIAM V. ROTH, JR., DEL., CHAIRMAN

CHARLES H. PERCY, ILL.
TED STEVENS, ALASKA
CHARLES McC. MATHIAS, JR., MD.
JOHN C. DANFORTH, MO.
WILLIAM S. COHEN, MAINE
DAVID DURENBERGER, MINN.
MACK MATTINGLY, GA.
WARREN B. RUDMAN, N.H.

THOMAS F. EAGLETON, MO.
HENRY M. JACKSON, WASH.
LAWTON CHILES, FLA.
SAM NUNN, GA.
JOHN GLENN, OHIO
JIM SASSER, TENN.
DAVID PRYOR, ARK.
CARL LEVIN, MICH.

JOAN M. MC ENTEE, STAFF DIRECTOR

SUBCOMMITTEE:
WILLIAM S. COHEN, MAINE, CHAIRMAN
TED STEVENS, ALASKA
WARREN B. RUDMAN, N.H.
CARL LEVIN, MICH.
DAVID PRYOR, ARK.
SUSAN M. COLLINS, STAFF DIRECTOR

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON
OVERSIGHT OF GOVERNMENT MANAGEMENT
WASHINGTON, D.C. 20510

August 24, 1982

The Honorable David A. Stockman
Director
Office of Management and Budget
Executive Office Building
Washington, D.C. 20503

Dear Dave:

On September 23, the Senate Subcommittee on Oversight of Government Management will hold a hearing on computer matching by government agencies to detect fraud or waste in government programs. The hearing will focus on the use of computer matching as a management tool, the cost-effectiveness of matching, and some public policy issues that may be raised by matching.

In order to assist the Subcommittee in its preparation for the hearing, I request that the appropriate official of the Office of Management and Budget provide the Subcommittee with the following materials:

A. 1) Copies of all matching reports submitted by agencies to the Director of the OMB pursuant to the OMB Guidelines for the Conduct of Matching Programs, issued by the OMB on March 30, 1979. Please supply the Subcommittee with all reports for both one-time matching programs and initial and renewal reports submitted to the OMB for continuing matches that were performed or proposed by agencies between the effective date of the March 1979 guidelines and May 1982, the effective date of the revised OMB guidelines.

2) Copies of all matching reports that have been submitted to the Director of the Office of Management and Budget pursuant to the requirements of the Revised OMB Guidelines for Conducting Computer Matches, issued May 14, 1982.

3) Copies of comments that were submitted to the OMB on proposed supplemental guidelines for Matching Programs pursuant to the Request for Comments published in the Federal Register on August 4, 1978.

4) Copies of the Office of Management and Budget's requests for comments on agencies' experiences or public comments on the proposed revision of the guidelines for computer matching programs prior to the May 1982 revision.

5) Copies of all comments received from federal agencies and other parties concerning the proposal to revise the computer matching guidelines in 1982.

B. In addition, please provide responses to the following questions:

1) What were the OMB's primary reasons for revising the computer guidelines in 1982?

2) Has the OMB ever advised a federal agency not to conduct a proposed matching project? If so, please describe the proposed matches and the basis for the OMB's objections.

3) What responsibilities, if any, for overseeing matching programs are given to the OMB under the Privacy Act and the Paperwork Reduction Act?

4) Should a cost-benefit analysis of computer matching be required prior to conducting a match?

5) Should agencies be required to report the results of the matching project, for example, the amount of money saved from the match, the number of cases being investigated or prosecuted, the number of cases dropped? If so, to whom should the agency report these results?

In order to allow the Subcommittee sufficient time to review this material prior to the hearing, I request that you provide the Subcommittee with your response no later than September 10, 1982. If a substantial number of comments have been filed with the OMB, I ask that you inform me of this so that my staff will be able to review the comments at the Office of Management and Budget and request copies of particular comments.

If you require further information, please have your staff contact Mary Gerwin or Susan Collins of the Subcommittee staff at 224-5538. Also, please provide the Subcommittee staff with the name of the appropriate person in your office who is responsible for this request. Please have your response mailed to the Subcommittee on Oversight of Government Management, Committee on Governmental Affairs, 3306 Dirksen Senate Office Building, Washington, D.C. 20510, or delivered to the Subcommittee office at 506 Carroll Arms, 301 1st Street, N.E.

I appreciate your assistance to the Subcommittee in its examination of computer matching.

With best wishes, I am

Sincerely,

Bill

William S. Cohen
Chairman

WSC:mbg

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

NOV [illegible]

Honorable William S. Cohen
Chairman
Subcommittee on Oversight of
Government Management
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

We have prepared the following attachments in response to questions set forth in Section A of your letter:

1) Copies of all matching reports submitted by agencies to the Director of the OMB pursuant to the OMB Guidelines for the Conduct of Matching Programs of 1979.

2) Copies of all matching reports that have been submitted to the Director of the Office of Management and Budget pursuant to the requirements of the Revised OMB Guidelines for Conducting Computer Matches, issued May 14, 1982.

3) Copies of comments that were submitted to the OMB on proposed supplemental guidelines for Matching Programs pursuant to the Request for Comments published in the Federal Register on August 4, 1978 are not available at this time. Those records have been retired.

4) Copies of the Office of Management and Budget's requests for comments on agencies' experiences or public comments on the proposed revision of the guidelines for computer matching programs prior to the May 1982 revision.

5) Copies of all comments received from federal agencies and other parties concerning the proposal to revise the computer matching guidelines in 1982.

Listed below are the responses to the questions raised in Section B of your letter.

1) What were the OMB's primary reasons for revising the computer guidelines in 1982?

   The matching guidelines were revised by OMB in the normal course of review of policy guidance issued to the agencies and as a result of numerous agency inquiries seeking interpretative guidance on their applicability and implementation.

2) **Has the OMB ever advised a federal agency not to conduct a proposed matching project? If so, please describe the proposed matches and the basis for the OMB's objections.**

   No.

3) What responsibilities, if any, for overseeing matching programs are given to the OMB under the Privacy Act and the Paperwork Reduction Act?

   OMB's authority to issue the matching guidelines stems from Section 6 of the Privacy Act which requires OMB to issue guidelines and regulations on the implementation of that Act and from the Paperwork Reduction Act which gives OMB federal information oversight authority and the responsibility to encourage data sharing among the agencies and to promote the effective use of information technology.

4) Should a cost-benefit analysis of computer matching be required prior to conducting a match?

   We think it is appropriate for agencies to use cost benefit analysis as one element in the decisional process. However, in justifying the initiation of a matching program, other elements should also be considered, e.g. deterrent effect. In any case, this is a management decision and is more properly left to the agency.

5) Should agencies be required to report the results of the matching project, for example, the amount of money saved from the match, the number of cases being investigated or prosecuted, the number of cases dropped? If so, to whom should the agency report these results?

The agencies are reporting the results of matching projects through the President's Council on Efficiency and Integrity in Government.

I hope the material we have prepared will be of assistance to you.

Sincerely,

David A. Stockman

David A. Stockman
Director

Enclosures

Note: Enclosures retained in subcommittee files.

AN EVALUATION OF NEW YORK STATE'S WAGE REPORTING SYSTEM:

The Real Cost of Computer Matching

Prepared by the Privacy Project
of the NYCLU Foundation*

December 1982

---

* This special report was prepared by Trudy Hayden, consultant to the Privacy Project of the New York Civil Liberties Union Foundation, and Norma Rollins, director of the Privacy Project.

BACKGROUND

The federal government's Project Match, initiated in 1977, was the forerunner of scores of computer matching systems set up at the state and federal levels to detect fraud in public assistance programs. From their inception, these programs have raised a host of privacy concerns, including the still unanswered question of whether such systems can be legally implemented under the provisions of the Federal Privacy Act.

What Project Match and similar programs do is electronically compare different computerized records. For example, a comparison of computer tapes of public assistance recipients with computer tapes of public and private payrolls may show that a number of the same names appear on both lists. These matches, or "hits," can then be investigated to determine whether they were receiving aid to which they were not entitled.

The number and complexity of such matching systems has grown dramatically, both because of computers' technological capacity to sift through millions of pieces of information in a matter of minutes, and because of growing zeal on the part of government officials and the public to reduce fraudulent or duplicate claims for public benefits. To date, unfortunately virtually universal acceptance of the aims of these programs has led to laxity in the demand for accountability.

There is no question that the goal of assuring that government benefits are paid only to those individuals legally entitled to receive them is a worthy one. However, there are serious questions concerning the cost and utility of computer matching programs in achieving this end. There is ample evidence that such programs have failed to achieve the monetary savings predicted and that any efficiency gained by the advent of these computerized matching systems has been far outweighed by the costs in terms of personal privacy.

* * *

Public resistance to a massive central government computer has been repeatedly manifest since the mid-1960's, when plans for a federal National Data Center were abandoned, largely because of fears about the impact on privacy. But today, the real danger lies not in the creation of large new physically centralized systems. Instead it lies in the quickening trend toward the linkage of separate data systems many of them long-established and accepted.

Everything which privacy advocates feared from a centralized data system can now be accomplished within a decentralized system whose component parts are linked to one another. In fact, the greater flexibility afforded by a decentralized but interconnected network of systems is likely to be even more detrimental to personal privacy than a single mammoth centralized system.

With such a network, information collected for one purpose becomes available for many different purposes. For example, the Department of Immigration and Naturalization Services recently requested access to the New York City Board of Education's computerized data bank of one million students. Their goal was to undertake an investigation of Spanish surname households in order to find illegal aliens.

The record search techniques developed to combat welfare fraud are systematically erasing the boundaries between separate personal data systems, creating so many exchanges, connections, disclosures and comparisons that for all practical purposes there will soon be no boundaries at all. Once the boundaries between different record systems have been erased, they cannot be reconstructed. But in the rush to root out fraud in government programs, these complex and subtle issues have not been debated seriously.

And there are already signs that the trend toward record-matching will go far beyond efforts to detect fraud. Already the Selective Service System is matching draft registration lists with the Social Security Administration and states' Motor Vehicle Department licensees' listings to find individuals who have not registered with the military.

We can easily imagine other uses which might be suggested by legislators at state and federal levels. For example:

* checking employment records against criminal and medical records as a way of weeding out certain ex-offenders, ex-mental patients or ex-addicts from certain kinds of jobs;

* matching tax returns against bank and credit card and other personal financial transaction records (a process which becomes more feasible with the expansion of electronic funds transfer services) as an efficient way of enforcing the tax laws;

* enabling creditors to track down defaulters by running matches of bad debt lists against employment records;

* identifying "problem" children by matching their rolls against child abuse registries, police and family court records, or mental health and drug treatment clinic records.

These only begin the list of possibilities, even without considering such obviously abusive purposes as political surveillance or hunting for social or sexual "deviants." Once the idea of computer matching has been accepted as a routine technique of law enforcement and public administration, it will be virtually impossible to draw any lines at all between "good" uses and "bad."

Privacy advocates have raised these considerations since the first computer matching system was proposed, but have to date been unsuccessful in moderating the pace of new systems development. However, now that matching has been in effect in some jurisdictions for several years, it is possible to begin to examine the facts about whether computer matching systems have actually served the purpose for which they were created -- uncovering fraud and saving money for the public. To this end, the New York Civil Liberties Union studied New York's largest matching program, the Wage Reporting System.

NEW YORK'S WAGE REPORTING SYSTEM

Enacted in 1978, New York's Wage Reporting System* is a quarterly computer match of public assistance and unemployment insurance rolls against the reported earnings of New York State's 8 million workers. New wage information is collected four times each year by the Department of Taxation and Finance, and matched against lists of public assistance recipients submitted by the Department of Social Services and of unemployment insurance claimants submitted by the Department of Labor. "Hits" are returned to the Departments of Social Services and Labor to be investigated for evidence of fraud.

The Wage Reporting System (WRS) was originally planned to run for three years. In 1981 it was extended for another three years, through March 1984, In their last annual report, dated February 1982, the Commissioners of Social Services, Labor, and Taxation claimed that WRS, in the last fiscal year, had saved $23.7 million in public assistance, and since its inception, $14.5 million in unemployment insurance.

On the basis of claims such as these, it has been widely assumed that the apparently simple process of matching records has saved New York's taxpayers many millions of dollars in fraud and abuse. On closer examination, however, the NYCLU believes that WRS is not cost-effective, and that the privacy of millions of New Yorkers has been endangered to very little purpose. Our analysis of the claims made for WRS suggests:

---

* Chapter 545, Laws of 1978.

- that the actual costs of operating the system are far greater than New York State admits;
- that there are many hidden costs to employers which have not been computed;
- that estimates of so-called "savings" include millions of dollars that in fact cannot or will not be "saved"; and
- that losses to public assistance and unemployment programs attributable to deliberate fraud and abuse could be detected by less cumbersome and wasteful means.

A. THE COSTS OF OPERATING THE WAGE REPORTING SYSTEM ARE HIGHER THAN NEW YORK STATE ADMITS

It is very difficult to determine how much WRS costs the State of New York to operate. The "state costs" listed in the annual reports for the first two complete fiscal years of operation are $5.8 and $6.7 million respectively, but the New York State budget earmarked appropriations for both those years are just under $11 million annually. However, the problems of estimating costs go beyond this evident discrepancy because it is clear that only a portion of the actual costs attributable to WRS are identified as such. For example:

- Neither in the annual reports nor in the New York State budget is there a special WRS appropriation for the Department of Labor. How can it be possible that the Department participated in the cross-matching of over 1.2 million unemployment insurance claimant records and audited nearly 67,000 cases* without spending one cent? Surely some portion of the Department's annual operating budget must be used to support its participation in WRS.

- The Department of Taxation and Finance, which houses WRS, received two separate earmarked appropriations totaling about $10 million in fiscal year 1980-81 and again in 1981-82. These "dedicated " costs - already considerable higher than the total "state costs" for those years given in the WRS annual reports -- appear to support only the basic ministerial operations of collecting and maintaining quarterly wage reports from employers, crossmatching records submitted by the Departments of Labor and Social Services, and returning wage data on "hits" to these departments. While DTF claims that its operating costs were substantially lower in 1981-82 and could be reduced by $1 million next year, we suspect that a good portion of that reduction is likely to be accomplished by transferring some of the costs to employers. In fact, announced plans for new matches using WRS will probably make its operation more expensive rather than less.

---

* Represents matches and completed investigations throu h the first quarter of 1980; see Fourth Annual Report, 2/1/82, p. 17.

- The Department of Social Services performs many complex computer operations and follow-up investigations in conjunction with WRS, but the New York State budget appropriates only about $500,000 annually for this purpose. We note that in 1980-81 DSS spent at least $115 million to run its welfare, Medicaid, and child support management and fraud investigation programs and that the Department's use of WRS has gradually been integrated with these larger systems. We believe that some of this $115 million represents the cost of DSS participation in the Wage Reporting System. The largest unaccounted cost is represented by the many thousands of hours required for administrators and caseworkers in the local social services districts to review, verify, and investigate the status of the enormous number of "hits" produced by each crossmatch -- at last count, over 90,000 for a single quarter.

- No information is available on the cost of conducting fraud investigations, or of subsequent prosecutions.

As the table that follows illustrates, taken all together, these unreported costs of operating the Wage Reporting System could easily add up to three or four times the $6.6 million officially put forward as the estimated annual "state costs" in 1981-82 and 1982-83.* No fair assessment is possible unless all costs incurred by WRS are disclosed. So far, New York State has not done so.

HIDDEN COSTS OF THE WAGE REPORTING SYSTEM

SYSTEM PARTICIPANTS	TASK	$ ALLOCATED IN 1981 NEW YORK STATE BUDGET	ACTUAL COSTS
325,000 + private and public employers in New York State	Submit quarterly reports on 8 million employees	no allocation	Unknown
	Provide additional details on "hits" being investigated by DSS and DOL	no allocation	Unknown
Department of Taxation and Finance	Quarterly crossmatching of 8 million employment records against DSS and DOL lists and forwarding of "raw hits"	approx. 10 million	Unknown
Department of Labor	Participate in crossmatch of 1.2 million claims	no allocation	Unknown
	Audit 67,000 cases	no allocation	Unknown
Department of Social Services	Participate in crossmatch of 1.2 to 1.8 million recipients each quarter	approx. 500,000	Unknown
	Initial screening of approximately 200,000 "raw hits" each quarter		
	Local districts investigate approximately 100,000 hits each quarter	no allocation	Unknown

This table indicates that no money was allocated in the New York State Budget to cover many major expenses of the Wage Reporting System, nor do the annual reports indicate the costs by agency and function. The February 1982 WRS report indicates the system cost $6.7 million. However, failure to account for expenses by category casts serious doubt upon the accuracy of this figure. The actual cost of all components of the program appears to be substantially higher.

B. THERE ARE MANY HIDDEN COSTS TO EMPLOYERS

Between 325,000 and 350,000 employers file wage reports each quarter. The State acknowledges that the success of WRS depends heavily upon the cooperation of the business community in filing timely and complete reports.

The contributions of employers may be much greater than anyone realizes. The Wage Reporting System was instituted just at the time when the Social Security Administration converted from a quarterly to an annual collection of wage data from employers, pursuant to Congressional legislation* recommended by the Commission on Federal Paperwork in order to realize an estimated $360 million (in 1975 dollars) savings to employers. New York's employers are not enjoying their share of these savings -- a higher figure, of course, in 1982 dollars.

Furthermore, the Wage Reporting System is not a mere duplication of reports that employers would have to compile for other purposes. The definitions of employees and wages to be reported are different from those required for tax reporting system. Compliance with WRS imposes discrete record-keeping and reporting tasks whose costs have not been computed.

---

* P.L. 94-202.

While the direct costs of quarterly reporting are unknown, it is evident that the Department of Taxation appreciates the benefits to its own operating budget when employers submit their reports on magnetic tape rather than written forms, and has strongly encouraged them to do so. This, of course, enables the Department to bypass expensive data-entry procedures. The growing number of employers who submit computerized data -- 3764 at last count -- may account for some of the predicted $1 million reduction in WRS operating costs next year,* but it should be understood that this would be accomplished by shifting the cost of data entry to employers.

The submission of wage data is not the only responsibility that WRS imposes on employers. Follow-up investigations to verify the identity of assistance recipients and the accuracy of reported wages and periods of employment oblige employers to respond to numerous requests for detailed earnings histories. We note that the New York City Human Resources Administration is now asking employers to provide two years of employment history for every recipient reviewed.**

The aggregate costs to employers of their participation in WRS must be acknowledged in any assessment of the system's costs and achievements, particularly in light of the credit given to WRS for any benefit employers derive from savings to the unemployment insurance program. Even if the burden on the individual employer is modest, the combined annual contribution to the operation of WRS from New York's 325,000 or more employers in unaccounted personnel costs could easily come to $30 million.

---

* Fourth Annual Report, 2/1/82, p.2.
** Fourth Annual Report, 2/1/82, p.3.

C. THE "SAVINGS" ATTRIBUTED TO THE WAGE REPORTING SYSTEM MAY INCLUDE MILLIONS OF DOLLARS THAT ARE NOT ACTUALLY "SAVED."

The Department of Social Services claims that the Wage Reporting System is responsible for a reduction in public assistance payments of $9.2 million in 1979-80, $20.6 million in 1980-81, and $23.7 million in 1981-82. It estimates a gross savings of $29.1 million for 1982-83.

The Department of Labor, as of December 1981, claims a cumulative savings of $14.5 million to the unemployment insurance program, consisting of $4.5 million credited to employer accounts for improperly charged benefits and $10 million attributable to future benefits that will not be paid because of penalties imposed on violators.

As with so many other aspects of WRS, it is difficult to understand how the published figures are derived. The data we have, however, raise questions about the method of calculating savings.

- Three categories are identified as the source of savings to the public assistance program: cases closed due to ineligibility, cases rebudgeted, and cases closed due to the client's failure to report for an interview after a WRS "hit." In the last quarter for which complete figures are published (3rd quarter 1980), such cases totaled 2675. How much money these actions actually saved depends on how long payments would have continued at their earlier levels but for WRS-generated investigations. A statement made by the Commissioner of Social Services suggests that the Department projects the savings on each case for 18 months into the future.* In fact, however, there has always been a high turnover of public assistance recipients, especially among the occasionally employed who go on and off the rolls for brief periods. It is seriously misleading simply to absorb cases closed in one fiscal year into the "gross savings" of the next. At the very least, the Department must explain its reckoning of the number of months of savings credited to each closed or rebudgeted case. Until it does so, "gross savings" figures cannot be objectively appraised.

- Just as it is a mistake to assume that a closed case would have remained open for 18 months, so it is a mistake to assume that a case, once closed, will remain so. The Department does not disclose how many closed cases are later reopened, or how many decisions to close or rebudget cases have been reversed in fair hearings.

---

* Legislative conference February 1981, chaired by State Assemblyman David Walsh and Angelo DelToro.

- It is not clear that the estimated savings in public assistance are attributed solely to WRS. Clients frequently fail to report for recertification interviews; is WRS credited with all of these? Rebudgeting is common for clients in marginal employment. Because of the substantial time lapse between an employer's submission of a quarterly wage report and a determination by local caseworkers, a case may have been closed or rebudgeted even before a WRS "hit" is investigated by the local district. On the basis of the published data, it is uncertain whether all of the case actions credited to WRS are justified.

- The Department predicts further savings through recoupment. However, substantial recoupment may not be possible where it would reduce assistance below a client's present need. No data are available to indicate whether effort at recoupment after a WRS "hit" have generated any actual savings.

- The "deterrent" effect of WRS has been predicted from the beginning. Such savings are of course unmeasurable, but seem to be belied by the steadily increasing numbers of reported cases closed and savings attained.

- More than two thirds of the reported savings to the unemployment insurance program consist of future benefits forfeited by violators. But these savings would be realized only if all the affected individuals came forward to claim further benefits. As yet there are no data indicating whether the Department of Labor has been able to collect repayments from violators who are now gainfully employed.

We do not dispute the fact that the Wage Reporting System has produced savings in the public assistance and unemployment insurance programs. We question whether some of the millions of dollars claimed as "savings" represent monies truly "saved," and note especially that the published data are not sufficient to permit a fair judgment.

D. LOSSES DUE TO FRAUD AND ABUSE COULD BE DETECTED BY LESS CUMBERSOME MEANS.

It would be wrong to think of computer-matching as a simple or efficient operation.

Each quarter, the Department of Social Services has been sending between 1.2 and 1.8 million records of public assistance recipients to the Department of Taxation. Each quarter, the Department of Taxation has been sending back about 10% of these as "hits." Of the "hits," from a third to a half or more are transmitted by the Department of Social Services to local districts for investigation; the rest, presumably, are identified as "mismatches" at this early stage. Ultimately, from 3 to 4% of cases referred for local investigation are closed or rebudgeted; about 0.1% are found to have been completely ineligible for benefits.

Investigations by local caseworkers are painstaking. They may require multiple contacts with clients and employers to verify the identity of the client and the amount of earnings, to match the dates of earnings and benefits received, and to recalculate the proper level of payment and any possible overpayment. The paperwork is formidable. Yet the number of cases finally affected is minute. Figures for the last fully reported quarter (3rd quarter 1980) illustrate this well:*

1.5 million records of public assistance recipients and absent parents were sent to be matched.

167,563 "hits" were sent back to the Department of Social Services.

68,927 "hits" were sent to local districts for investigation.

2,675 cases were rebudgeted or closed:

1,965	rebudgeted for undisclosed amounts
624	closed for failure to report
86	closed as ineligible

It is also reported that 1667 cases were referred for fraud investigation, but no figures are given on the number of suspected fraud cases confirmed.

Obviously, there is a great deal of wasted effort here. An enormous number of computer "hits" are identified immediately as mistakes. Over 95% of the cases investigated locally are either mismatches or found not to involve unreported earnings. A significant portion of the rest are closed only because the client does not cooperate in the investigation, and even where unreported earnings are found, the greatest number of cases are rebudgeted rather than closed altogether. Only a very small number of clients are found to have earned too much to qualify for any assistance at all: in one quarter, 86 out of one and a half million people.

---

* Fourth Annual Report, 2/1/82, p.14.

We have many questions about the efficiency of the Wage Reporting System even beyond the absurdity of these numbers. For example:

- How large are the amounts overpaid? If only a small proportion of cases involve substantial amounts, other methods of detection may be just as effective and far more efficient. If many cases result in only minor revisions, the cumbersome machinery of WRS may be a classic case of "overkill."

- How many cases of actual fraud are there? How many overpayments result from administrative error or from a client's unintentional mistake? The very large number of verified "hits" that do not lead to an adverse determination reflects the fact that many people who earn some money are still eligible for benefits. The absence of any data on the outcome of fraud investigations resulting from WRS "hits" makes it impossible to judge whether computer-matching really does protect against client fraud.

- The Wage Reporting System may be better than nothing, but how does cost control by computer-matching compare to other methods? Would random audits produce equivalent results: could DDS devise internal administrative and accounting methods that would provide more reliable indicators of possible fraud? Is client fraud the major source of waste in public assistance programs? Might both fraud and waste be reduced even more by simplifying the rules for determining eligibility and calculating benefits? The mere assertion that WRS saves money is not proof that it is the most efficient and cost-effective way to save money.

CONCLUSION.

The mystique of computer-matching has achieved widespread appeal. Somehow, the apparently simple procedure of matching two databanks and spitting out "hits" seems like the "logical" and "scientific" answer to complex management problems. We submit, however, that the Wage Reporting System in New York State is an extraordinarily clumsy and wasteful operation, that it costs far more and saves far less than its propoents claim, and that the creation of a major threat to the privacy of millions of employed and unemployed New Yorkers cannot be justified as a "cost-effective means of controlling fraud and abuse."*

Finally, we submit that our predictions of the inevitable growth of the Wage Reporting System beyond the limits of its original purpose have been realized.** In addition to public assistance and unemployment insurance, WRS matches are being performed in the child support, Medicaid, and food stamp programs and to locate sources of third party health insurance for Medicaid recipients; matches are planned for the day care program; preparations are under way to integrate federal payroll data into WRS.* WRS is clearly envisioned as the core of an enormous system of social services management by electronic surveillance. We caution that as the Wage Reporting System grows larger, it will become even more expensive and less cost-effective than it is today, and the citizens of New York will see their right to privacy diminished even further in return for minimal gains to the public treasury.

---

* Fourth Annual Report, 2/1/82, p.ii.

** NYCLU Legislative Memorandum #9, 1978.

---

* Fourth Annual Report, 2/1/82, pp.3-7, 11-12.

THE STATE OF WYOMING

ED HERSCHLER
GOVERNOR

Department of Health and Social Services

Office of the Director

HATHAWAY BUILDING
CHEYENNE, WYOMING 82002
TELEPHONE (307) 777-7656
TTY 777-7385

22 AM 9 51

November 16, 1982

Hon. William S. Cohen, Chairman
Subcommittee on Oversight of
Government Management
United State Senate
Washington, DC 20510

NOV 22 '82

Dear Chairman Cohen:

This is in reply to your letter dated November 8, 1982, regarding hearings on computer matching by government agencies to be held on December 15 and 16, 1982.

Our experiences with computer matching have been good. We presently match Aid to Families with Dependent Children (AFDC) and food stamps against our state's wage file on a quarterly basis. Our Child Support Enforcement (CSE) unit matches with Employment Security Commission's (ESC) wage file ad hoc through written requests. However, CSE is in the process of arranging with ESC to access their Unemployment Insurance Benefits (UIB) file through an inquiry process online. When that is accomplished, we would like AFDC and food stamps to access UIB as well as wages. CSE also matches with IRS to tap tax refunds of absent parents. We once conducted an ad hoc match with the State of Wisconsin and found four matches from a small random sample.

The result of the Wisconsin match was that two of the four were paid twice (once by the State of Wyoming the month the recipient(s) left and by Wisconsin the same month.) However, our statute allows payment for the month they leave, and Wisconsin apparently has no waiting period, so recovery was not pursued. Matching allowed child support to recoup 104% of their targeted amount. Food stamps and AFDC continue to match with ESC's wage file on a quarterly basis and indeed find it helpful (even though they have not calculated an exact percentage at this time.) The current matches cost between $200 and $500 per month. However, the front end programming cost has been deterred up to this time. We hope to begin using some user friendly programming languages which would avoid system development costs and encourage more matching in the future.

We established a recovery unit in July 1982 and hope to expand that single position to a team of at least two; then computer matches would prove even more beneficial. Currently the investigation has to be conducted by our workers in the county offices and, frankly, with economic conditions the way they are, those same workers are already working under a heavy burden. We hope to use computers and office automation wisely so that we can alleviate the current workload; THEN we hope to incorporate more computer matches and more recoupment of funds and avoidance of errors.

Thank you for the opportunity to let you know what our state is doing in the field of computer matching.

Sincerely,

Stanley H. Torvik

Stanley H. Torvik
Director

mm

cc: Sen. Malcolm Wallop
Sen. Alan K. Simpson
Rep. Dick Cheney

PS: We have made arrangements to obtain the two computer programs for matching social security numbers. These will be programmed onto our CPT equipment as soon as practicable. (Offered by the Inspector General's office.)

JOSEPH E. BRENNAN
GOVERNOR

WILLIAM R. MALLOY
COMMISSIONER OF LABOR

SETH W. THORNTON
EXECUTIVE DIRECTOR

STATE OF MAINE
DEPARTMENT OF LABOR
BUREAU OF EMPLOYMENT SECURITY
POST OFFICE BOX 309
20 UNION STREET
AUGUSTA, MAINE 04330

November 19, 1982

Senator William S. Cohen
Subcommittee on Oversight of Government Management
Committee on Governmental Affairs
3306 Dirkson Senate Office Building
Washington, D. C. 20510

Dear Senator Cohen:

In response to your inquiry of November 8, 1982, relative to the use of computer matching, the following is submitted:

The Maine Department of Labor maintains computer files and histories of all claims for unemployment benefits. Computer files of the wages of all workers in covered employment are also maintained. These two (2) files are utilized for all matching activity.

The claims history file and the wage file are compared each quarter to detect possible fraudulent unemployment benefit claims. The output of this match, and subsequent investigation, identifies approximately $75,000.00 per quarter erroneously paid in unemployment benefits to approximately 400 claimants. Collection actions are taken to recover this money.

The Department of Human Services requests a match of their AFDC and Food Stamp client files and our files each quarter. This match is to detect fraud and unreported income.

Individual matches are made daily for the Department of Human Services to assist them in determining client eligibility for AFDC and Food Stamp assistance.

The computer output of matches performed for the Department of Human Services is given directly to that department, therefore, this Agency has no record of the effectiveness of the program.

Costs for performing the matches cannot be determined with the computer currently used. It is so old that cost accounting software is not available for it. Since the system was paid for years ago, estimates of cost would not be realistic.

The match to identify erroneous unemployment benefit payments is the most successful we conduct.

An Interstate match of benefits and wages is currently being developed by the U. S. Department of Labor. This program will further enhance our ability to detect fraud or overpayments.

Current safeguards to protect the confidentiality of records are in accordance with Federal guidelines and are deemed adequate.

The Department's present computer system is inadequate for our needs. The Agency is in the process of acquiring new computer system capabilities.

Maine data files contain high quality and complete data records.

If we may be of further service to you, please advise.

Very truly yours,

Seth W Thornton

Seth W. Thornton
Executive Director

WV:nlc

JAMES A. RHODES
Governor
State of Ohio

KENNETH B. CREASY
Director
CHARLES E. NOGGLE
Assistant Director

DEPARTMENT of PUBLIC WELFARE

OFFICE OF THE DIRECTOR
30 East Broad Street
Columbus, Ohio 43215

-1 [illegible] 10:38

November 24, 1982

The Honorable William S. Cohen, Chairman
Subcommittee on Oversight of Government Management
Committee on Governmental Affairs
3306 Dirksen Senate Office Building
Washington, D. C. 20510

DEC 1 '82

Dear Senator Cohen:

We are in receipt of your letter of November 8, 1982 regarding computer matching to prevent and detect fraud and waste in federal and state welfare administered programs.

Ohio has been engaged in computer matches for a number of years. Some matches are done monthly; for example, Bureau of Employment Services. We also do quarterly matches with a variety of agencies, and have done some one-time-only matches with private industries.

Ohio has statistics from the April 1978 SSA match on the amount of under/overpayments discovered through the match. These figures involve all incorrect payments that occurred in these cases, and could include one month or two years of these payments.

Out of 53,840 matches reviewed:

46,620 (86.6%) were matches involving no errors.

7,220 (13.4%) were matches involving incorrect payments totaling an estimated $36,345 in underpayments and $8,996,405 in excess payments.

Out of the 53,840 matches reviewed:

46,620 (86.6%) were matches involving no errors.

2,056 (3.8%) were matches involving incorrect payments but no intentional client errors.

5,164 (9.6%) were matches involving incorrect payments and suspected intentional failure to report income.

Senator William S. Cohen
Page 2
November 24, 1982

There are no statistics available on how many cases suspected of intentional failure were found guilty of fraud, or on how much money was recovered on these cases.

The estimated computer cost is $65 per match. We do have some statistics based on the SSA earnings match which indicate a cost of $18 per item investigated.

Ohio feels that matches should be pursued as a deterrent and high priority given to developing and maintaining files of income and resource data so that a front-end edit can be used. It is more cost-effective to prevent improper payments than attempting to recoup overpayments. We are planning to pursue matches that we feel will provide the tools for prevention as well as follow-up, given the availability for funding and staff time.

We hope this information will be helpful to you.

Sincerely,

KENNETH B. CREASY
Director

KBC:blb

STATE OF CALIFORNIA—HEALTH AND WELFARE AGENCY

DEPARTMENT OF SOCIAL SERVICES
744 P Street, Sacramento, CA 95814
(916) 924-2836

November 30, 1982

Subcommittee on Oversight of Government
Management
Senate Committee on Governmental Affairs
3306 Dirksen Senate Office Building
Washington, D.C. 20510

Attention: Mary Gerwin or Susan Collins

The following information is provided in response to Senator Cohen's November 8, 1982 letter requesting information on the use of computer matching of records to detect fraud or waste in federal or state administered programs.

I have attached a brief summary of the major computer matching programs operated by our Department. Two of our programs, Project Intercept and Asset Clearance Match, utilize state income tax files and have definite possibilities of being expanded to the use of federal income tax files.

We feel that computer matching is an extremely useful tool and have ideas for other possible matches whenever data processing and personnel resources become available. We do operate under a handicap in our state due to the lack of a statewide welfare information system. Since California has a state supervised, county operated welfare system, most of the data needed for efficient computer matching only exists at the county level.

I hope that this information will be of value to the subcommittee. If you have any questions or desire additional information please contact me at (916) 924-2828.

Sincerely,

Mickey F Bach
for Larry L. Harrison, Chief
Welfare Fraud and Audits Branch

Attachment

DEC 6 '82

1. Earnings Clearance System (ECS)

Purpose = To identify unreported earnings of employed welfare recipients.

Jurisdictions = California State Department of Social Services and State Employment Development Department.

Match Identifier = Social Security Number

Frequency = Quarterly

Output = Welfare recipient's quarterly earnings as reported by their employers.

Cost Savings = Identifies approximately $12 million per year in welfare overpayments as a result of unreported earnings.

Costs = Approximately $50,000 per year.

2. Nevada Earnings Clearance System

Purpose = To identify unreported earnings of California welfare recipients employed in the State of Nevada.

Jurisdictions = California State Department of Social Services and Nevada State Employment Security Department.

Match Identifier = Social Security Number

Frequency = Annual

Output = Welfare recipient's earnings as reported by employers in Nevada.

Cost Savings = Identifies approximately $20,000 per year in welfare overpayments as a result of unreported earnings.

Costs = $7,800 paid to the State of Nevada, balance of costs included in the normal ECS production costs.

3. Project Intercept

Purpose = To intercept taxpayer's state income tax refund checks to recoup delinquent restitution of welfare overpayments.

Jurisdictions = California State Department of Social Services (SDSS) and State Franchise Tax Board (FTB).

Match Identifier = SSN and first four letters of last name.

Output = Identification of taxpayers having refunds intercepted and monthly fund transfers of intercepted amounts.

Cost Savings = Over $280,000 was collected in 1982. Expansion of the system should result in over $1 million being collected during 1983.

Costs = $36,000 (SDSS Computer Processing and Operations Support). FTB costs are unknown since SDSS accounts are combined with those submitted by approximately 70 other state agencies.

4. Asset Clearance Match

Purpose = To identify unreported assets (bank accounts, stocks, bonds, etc.) belonging to welfare recipients.

Jurisdictions = California State Department of Social Services and State Franchise Tax Board.

Match Identifier = SSN

Output - All accounts under the recipient's SSN that have been reported to the State Franchise Tax Board as having earned interest or dividends. (State law limits the output to only those cases where total interest/dividends is at least $30.)

Costs/Savings = Unknown at this time. Project began in October 1982.

3 04

STATE OF ILLINOIS
DEPARTMENT OF PUBLIC AID

DEC 6 '82

JEFFREY C. MILLER
DIRECTOR

316 SOUTH SECOND STREET
SPRINGFIELD, ILLINOIS 62763

December 1, 1982

The Honorable William S. Cohen
Subcommittee on Oversight of
Government Management
Committee on Governmental Affairs
3306 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Cohen:

In response to your November 8, 1982 request for comments on computer matching, enclosed is a comprehensive report of computer matching activities by the Illinois Department of Public Aid through 1981. We would like to expand our matching program to include wage and unemployment insurance information from other State's labor agencies, income/tax return information from the Federal Internal Revenue Service, and registration information from the U.S. Immigration and Naturalization Service. Unfortunately, access to some of this information is restricted by State and Federal legislation.

Thank you for the opportunity to provide comments to the Subcommittee. If you have any questions, please contact Mark Camille at 217/782-1128.

Sincerely,

Jeffrey C. Miller

Jeffrey C. Miller
Director

JCM:rj

ENCLOSURE

Illinois Department of Public Aid

DATA EXCHANGE SUMMARY
AS OF JANUARY 1, 1982

BACKGROUND & METHODOLOGY

The Illinois Department of Public Aid's (IDPA) Data Exchange Program has two major goals; 1) detecting ineligible or overpaid recipients and terminating or reducing their assistance, as appropriate, and 2) providing information on responsible relatives to assist our Bureau of Child Support in the search for absent parents and collection of support payments under Title IV-D.

Information provided by outside organizations is used to cross-check by computer Illinois recipient eligibility factors such as undisclosed assets and/or resources, unreported income, changes in employment status, changes in marital status, school attendance, and the number of people living in the household. The match criteria for most of the data exchanges conducted by the Illinois Department of Public Aid are first, all nine digits of the Social Security Number, and second for those persons not matching on SSN, the first four digits each of the first and last name, plus all six digits of the date of birth. The actual programming is done in Cobol language for use on an IBM 370 computer. The single data base utilized for the matches includes AABD, AFDC and General Assistance populations throughout Illinois. Those programs developed for use with the Illinois data base would not be easily utilized by other organizations unless their data bases were constructed in exactly the same manner as Illinois'.

TYPES OF DATA EXCHANGES

INTERSTATE DATA EXCHANGES	MONTH/YEAR RUN
1) Indiana	8/76, 3/78, 7/81
2) Michigan	8/76
3) Missouri	10/76
4) Mississippi	2/77, 9/77, 6/78, 5/79
5) Ohio	6/77, 9/78, 7/79, 10/80
6) Iowa	11/77
7) Project Match Interjurisdictional (HHS)	5/78, 12/78, 9/79
8) Arkansas	6/78
9) Bendex Interstate	10/78, monthly thereafter
10) Kentucky	11/78, 5/81
11) Wisconsin	9/79, 11/80, 9/81

Interstate Data Exchanges have been conducted since August, 1976 for the purpose of identifying recipients who are receiving assistance simultaneously in Illinois and another State. These matches have resulted in 592 negative actions (case cancellations or decreases in assistance), 56.0% of the 1,057 reviews completed with monthly grant dollar savings of $56,396.23. Also included in the Interstate totals are three Project Match-Interjurisdictional Projects initiated by the Department of Health and Human Services. States are initially selected for matches based on their geographic location relative to Illinois and/or the volume of Illinois recipients who previously resided there. The frequency of Interstate matches is dependent on past results and the availability of the information from the other State.

PUBLIC SECTOR EMPLOYER DATA EXCHANGES	MONTH/YEAR RUN
*1) Governmental Through U.S. Attorney	5/77
2) Chicago Crossing Guards	5/77
3) St. Louis & E. St. Louis Postal Employees	5/77
4) IL Dept. of Personnel (State Employees)	7/77, 2/78, 10/78
5) IL State Employees	8/77, 7/79, 1/80, 2/80, 1/81, 7/81
6) IL Municipal Retirement Fund (Contributors)	9/77, 11/77, 6/78, 7/78, 10/78, 3/79, 10/79, 1/80, 8/81
7) City of St. Louis Employees	10/77
8) Cook County Hospital Employees	10/77, 9/79, 3/80, 7/81

*Included numerous payrolls from departments in Chicago

PUBLIC SECTOR EMPLOYER DATA EXCHANGES (continued)	MONTH/YEAR RUN
9) IL Dept. of Public Aid Employees	3/78
10) Project Match Federal Employees	4/78, 6/80
11) East St. Louis Employees	4/78, 2/79
12) Chicago Housing Authority Employees	9/78
13) New Public Aid Employees	9/78
14) Cook County Board Employees	10/78, 3/80, 11/81
15) Chicago Sanitary District Employees	10/78, 4/79
16) Chicago Transit Authority Employees	3/79, 6/81
17) Chicago City Employees	5/79, 10/79, 3/80, 9/80
18) Chicago Board of Education Employees	3/80

Public Sector Employer Data Exchanges have been conducted since May, 1977 to identify recipients who were employed and not reporting some or all of their income to the Department. These matches have resulted in 5,418 negative actions, 43.3% of the 12,504 reviews completed. Monthly grant dollar savings of $969,487.00 have been achieved from these Public Sector Employer Data Exchanges.

The Public Sector Employer Data Exchanges which have proven to be cost-beneficial are now set up to run on one of three cycles; quarterly, semi-annual, or annual, based on the effectiveness of the matches and the agreements established with the participating organizations.

PRIVATE SECTOR EMPLOYER DATA EXCHANGES	MONTH/YEAR RUN
1) St. Mary's Hospital Employees	6/77
2) Barnes Hospital Employees	8/77
3) Spiegel Employees	8/77
4) St. Louis University Hospital Employees	10/77
5) John Deere Employees	11/77
6) American Motors Corp.-Kenosha Employees	12/77
7) Taxicab Drivers	2/78, 9/78
8) U.S. Steel Employees	2/78
9) McDonnell-Douglas Employees	6/78
10) Mt. Sinai Hospital Employees	12/79
11) Sunbeam Employees	1/80
12) Rush Presbyterian Hospital Employees	4/80
13) IC Industries Employees	3/81

Private Sector Employer Data Exchanges were initiated in June, 1977 to identify recipients who were employed and not reporting some or all of their income to the Department. These data exchanges have resulted in 432 negative actions, 596% of the 725 reviews completed. Monthly grant dollar savings of $80,248.43 have been achieved in 13 Private Sector Employer Data Exchanges.

It has become increasingly difficult to conduct the Private Sector Employer Data Exchanges due to employer reluctance to release information to the Agency and lack of response to our initiating letters. Several employers have cited confidentiality restrictions which prevent them from forwarding payroll files.

OTHER ELIGIBILITY FACTOR DATA EXCHANGES	MONTH/YEAR RUN
1) IL Public Health Deaths	6/76, 4/80, 8/80, 10/80, 3/81, 4/81, 8/81, 11/81
2) Intrastate Duplicate Recipients	7/77, 12/77, 3/78, 7/78, 12/78, 7/79, 12/79, 3/80, 5/81, 9/81, 11/81
3) Reinstated Data Exchange Cancellations	10/77, monthly thereafter
4) IL Department of Corrections (Inmates)	2/78
5) St. Clair County General Assistance Rolls	3/78
6) General Assistance Childbirth	8/78
7) Chicago Board of Ed.-Children Sample	8/78, 6/80
8) IDPA Escheated Warrants	9/78
9) IL Secretary of State Motor Vehicle	2/79
10) Public Health Marriage License	2/79, 11/79, 2/80, 8/80, 1/81, 3/81
11) Chicago Assessor (Vacant Lots)	3/79
12) IL Comptroller Tax Refund	4/79
13) Summary Earnings Record Sample (HEW)	4/79
14) Multiple Assistance Cases At One Address	12/80
15) Data Exchange Cases Previously Identified 3 Or More Times	4/81
16) Responsible Relative in Home	9/81

Other Eligibility Factor Data Exchanges begun in June, 1976 are designed to identify a broad spectrum of potential errors, e.g., intra-State duplicate recipients, unreported deaths and marriages and unreported assets. A total of 6,298 negative actions have been processed from 11,827 reviews completed. This represents a 53.3% negative action rate and has been responsible for monthly grant dollar savings of $783,342.38. A review of the Other Eligibility Factor Data Exchanges for effectiveness in eliminating ineligibility and overpayment has resulted in some of them being discontinued. The remaining data exchanges are set up to run on a monthly, quarterly or semi-annual basis.

ILLINOIS DEPARTMENT OF LABOR

The Illinois Department of Public Aid conducts two data exchanges based on benefits and earnings information received from the Illinois Department of Labor. A quarterly data exchange utilizing Illinois Department of Labor earnings information was initiated in 1975 to identify employed recipients who were not reporting some or all of their income to the Department of Public d. In addition, the Department of Labor in 1978 began providing Unemployment Insurance Benefit information on a monthly basis which has been utilized to identify recipients failing to report some or all of their benefits. Matches must have at least a 15% difference between benefits or earnings reported to the Agency and those issued to the client according to Labor before they are identified for investigation. A total of 74,053 negative actions have been processed from the 247,347 reviews completed. This represents a 29.9% negative action rate and has resulted in monthly grant dollar savings of $12,285,314.00.

ERROR PROFILING

The development of criteria to assist field staff in redetermining the caseload dates back to early 1975 when error profiles were constructed for AFDC and General Assistance cases. The sources for the profiles, developed using discriminant analysis and multiple regression, were the January-June, 1974 Quality Control samples. The profiles were utilized monthly from December, 1975 through October, 1981 to identify error prone recipients. These data exchanges have resulted in 18,147 negative actions, 34.0% of the 53,311 reviews completed. Monthly grant dollar savings of $1,877,566.00 were achieved.

NEW INITIATIVES

During 1981, the Department initiated data exchanges designed to locate responsible relatives and to identify third party liability resources.

Six responsible relative (IV-D) matches were conducted in 1981, which assisted our Bureau of Child Support in their effort to locate relatives and then collect legally mandated child support payments when appropriate.

In the area of Third Party Liability, a data exchange was conducted between Department of Public Aid and Department of Personnel records to identify Public Aid recipients employed by the State of Illinois who are covered by Blue Cross/Blue Shield Health Insurance. This information was to be utilized by the Third Party Liability Unit in identifying medical bills previously paid by Medicaid, which could potentially be recouped from Blue Cross/Blue Shield.

NEGATIVE FACTORS

While the data exchange program has been largely successful in achieving its goals of identifying ineligible and overpaid recipients and providing the Bureau of Child Support with updated information on responsible relatives, some negative aspects have been encountered which prevent the Data Exchange Program from achieving its full potential. These aspects can be placed in six categories: 1) Differences in computer hardware between the Illi. 's Department of Public Aid and the participating organization, 2) Receipt of an unreadable or unusable tape from the participating organization, 3) Lengthy turnaround time by our Bureau of Information Systems staff caused by unfamiliarity with the requested data or backlogs in project scheduling, 4) Food Stamp Only cases not being available to be matched because Social Security Numbers and Birthdates are not contained on our data base, 5) Data Exchanges which save less than the cost of production or are unsatisfactory for other reasons, and 6) Organizations which decline to participate in the Data Exchange Program. Reasons for not participating can generally be characterized under the following headings:

1) Non-Response to initiating letter sent by the Agency or failure to send data after agreement established,
2) Computer problems (not computerized, incomplete computer system),
3) Confidentiality restrictions,
4) Preferred Federally sponsored Interstate Match, or
5) Conditions for providing data were unacceptable to the Agency.

Non-participation has affected all four groups of data exchanges, particularly those proposed with Public Sector and Private Sector Employers. Twelve (12) Public Sector and fourteen (14) Private Sector Employer matches were never conducted due to the conditions described previously. Also, five (5) Interstate Data Exchanges and six (6) Other Eligibility Factor Data Exchanges were not scheduled for one of the five reasons. In the latter category, proposed data exchanges with the Illinois Departments of Mental Health, Corrections, Law Enforcement and Revenue were never completed due to confidentiality restrictions.

A few data exchanges in each of the four groups have saved less than the cost of production or have been unsatisfactory for other reasons. These reasons are as follows:

1) Low Volume of Matches (Mississippi IV-D, Department of Conservation IV-D, and Cook County Hospital IV-D),
2) Operational Problems (Project Match Interjurisdictional Phase III), and
3) Lack of Federal Agency Cooperation (Project Match Federal Employees - Phase III).

CONCLUSION

In summary, although the Data Exchange Program has been unable to totally achieve its goals because of the negative factors outlined previously, it continues to be a positive tool in the Agency's efforts to reduce ineligibility and overpayment and to collect legally mandated child support benefits on behalf of AFDC recipients. Future plans for the program include the initiation of at least one new data exchange proposal each month, as well as the continuation of efforts to address problems in three areas:

1) Recipient (IV-A) Eligibility,
2) Location of Responsible Relatives (IV-D), and
3) Identification of Third Party Liability.

STATE OF MICHIGAN

WILLIAM G. MILLIKEN, Governor
DEPARTMENT OF SOCIAL SERVICES 59
300 South Capitol Avenue, P.O. Box 30037, Lansing, Michigan 48909
[illegible]
Noble P. Kheder, Director

December 6, 1982

The Honorable William S. Cohen, Chairman
Committee on Governmental Affairs
Subcommittee on Oversight of Government Mgmt.
United States Senate
Washington, D.C. 20510

Dear Senator Cohen:

This letter is in response to your request dated November 8, 1982 for data regarding match project activity by our Department.

We maintain the two on-going systems of BENDEX and SDX. In addition we conduct periodic wage/benefit matches with both private employers and other governmental agencies. Most notable has been the matches with the auto industry.

Though savings have been considerable through use of match projects, specifics are difficult to pinpoint. For example, we closed or reduced over 500 grants in our auto industry project resulting in a monthly savings of over $125,000. However, the costs associated to field staff time necessary to verify and take action on the computer match data is unavailable. This cost represents the most significant expenditure next to the one time only systems developmental costs.

The most successful match projects are the ones which associate current wage or benefit data to current eligibility. The longer the time span between the wage or benefit data and the eligibility period in question, the more field staff time necessary to review and corroborate data.

Optimally, computer match efforts become most effective when employed in a network environment. This technique would link all requisite information resources (e.g., Treasury, Labor, etc.) and subsequently become available for use by the welfare agency at either time of initial application or redetermination. This would promote a minimal, consistent delay under most circumstances, between the time the welfare agency becomes aware of information in conjunction to the time the recipient or applicant files the information.

Our data processing capabilities would be sufficient to accommodate most match project efforts. However, much of the data vital to the success of such efforts is gathered by other governmental agencies who are either precluded by law from disclosing same or who do not encode the information for use on an automated system. To relieve this bottleneck would require enhancements in law and funding sufficient to reimburse other governmental agencies for costs incurred in gathering and processing data vital to continuing welfare eligibility determination efforts. In addition, there should certainly be available Federal financial incentives to states without adequate systems capability or support.

Certainly, every effort must be expended to insure the integrity of the individual's right to privacy. However, consideration must also be extended modern technology and its use in maintaining the integrity of the various benefit programs. To do otherwise would certainly result in needless expense and information management chaos.

We hope the questions raised have been addressed. Should you have need of additional information, please contact me at your convenience.

Sincerely,

Noble P. Kheder

Arkansas Department of Human Services
Division of Social Services
Seventh and Main Streets
P.O. Box 1437
Little Rock, Arkansas 72203

Frank White
Governor

Ray Scott
Director

[illegible] PM 12:01

December 6, 1982

The Honorable William S. Cohen, Chairman
Subcommittee on Oversight of
Government Management
3306 Dirksen Senate Office Building
Washington, D.C. 20510

[illegible] '82

Dear Senator Cohen:

The attached sheet provides estimates of the costs and benefits associated with our various match activities. Because of the immediate need for this information, more detailed cost information was not available.

As you can see, the most effective efforts have been the Wage/Unemployment Benefit Match for AFDC and the Child Support Match with the Internal Revenue Service.

We believe that computer matching is an effective management tool and expansion should be encouraged. Additionally, we feel that States should be encouraged to enhance their computer systems to facilitate more matches and to improve the quality of such matches. Incentives, such as improved match rates for computer development should be considered.

Present safeguards regarding confidentiality of records appear adequate. In fact, we would suggest that these safeguards be reviewed to determine if they are too restrictive and impede the effective operation of computer matches.

We appreciate the opportunity to comment on this issue and hope that this information proves useful to you.

Sincerely yours,
Dorothy K Rappeport
Dorothy K. Rappeport
Commissioner

DKR:sb

Attachment

"The Arkansas Department of Human Services is in compliance with Titles VI and VII of the Civil Rights Act and is operated, managed and delivers services without regard to age, religion, handicap, sex, race, color or national origin."

ARKANSAS SOCIAL SERVICES

MATCH SUMMARY

Program	Match Type	Estimated Annual Cost	Estimated Annual Savings
AFDC	Wage/Unemployment Benefits	5,600	$1,828,488
AFDC	Interjurisdictional Match	Not Available	63,086
Food Stamps	Wage/Unemployment	51,000	100,000
Food Stamps	State Data Exchange	Not Available	60,000
Child Support	Internal Revenue Service	Not Available	600,000
Child Support	Revenue Department	Not Available	Not Available
Child Support	Employment Security Division	$24,000	Not Available
Child Support	Criminal Information System	Not Available	Not Available

STATE OF CONNECTICUT
DEPARTMENT OF INCOME MAINTENANCE

[illegible] AM 10:10

GEORGE B. COLEMAN
DEPUTY COMMISSIONER

TELEPHONE
(203) 566-2759

December 8, 1982

Senator William S. Cohen
United States Senate
Committee on Governmental Affairs
Washington, D. C. 20510

DEC 14 82

Dear Senator Cohen:

In response to your letter of November 8, 1982 regarding utilization of computer matches in the Connecticut Department of Income Maintenance, we submit the following comments:

(1) We are in the process of or have conducted a number of matches:

- Labor Department
  AFDC cases are matched quarterly and we have on-line capability.
- Interjurisdictional with Rhode Island and bordering New York counties. (once a year)
- AFDC cases that have more than one date of birth for family members that match with another case (routine)
- VA against State Aged, Blind and Disabled Program to determine income discrepancies (routine)
- Three or more Public Assistance checks going to the same address (routine)
- Bendex (routine)
- Match with General Assistance caseload (being developed)
- AFDC children with School Records (being developed)
- Bank match - entire caseload (planned)
- Medicaid Eligibility File against BC/BS (being developed)
- On line access to Motor Vehicle files (being developed)

2. Except for the Labor Match, costs savings are difficult to determine. The Labor Match has little impact on current eligibility as wage records are 3 - 6 months old, client is determined presently unemployed and few cases can be discontinued or modified. However, we do uncover past overpayments. For example, between 8/1/80 and 5/31/81, 661 cases were referred for fraud in the amount of $614,000 - all directly uncovered through use of Labor files. About $100,000 is in the process of being recouped.

STATE OF CONNECTICUT
DEPARTMENT OF INCOME MAINTENANCE

GEORGE B. COLEMAN
DEPUTY COMMISSIONER

TELEPHONE
(203) 566-2759

Interjurisdictional matches result in few savings - frequently less than half a dozen cases (out of 44,000) are discovered as a result of this match.

(3) Computer costs are minimal (e.g. Labor Match costs $300 per month) but staff time to investigate findings, given already limited resources) is prohibitive. Although there is a psychological, deterrent factor to fraud in some of these matches, we need to be most selective in using this method for reducing errors.

(4) If Labor files were updated in a more timely fashion, this would be the most successful match.

(5) Again, computer matches should be limited to those that are most cost effective and should not be used generally to replace traditional procedures for determining eligibility and correctness of payment.

Internal matches between programs are simplest and do help detect inconsistencies without endangering confidentiality.

External matches require the most intensive work, are costliest and do raise confidentiality issues. We have found this issue to be problematic when trying to reach matching agreements with banks and other state agencies, both of whom are fearful that misues of information will adversely affect their client population. One way to resolve this problem is through formal, detailed inter-agency agreements relative to computer matches.

(6) The biggest problem investigating matches is the validity of file information differently compiled, so that Social Security number is frequently the only element on which a match can be made. The greatest number of mismatches occur because of an incorrect number on file. Matching project could be simplified if matches could be made on three or four elements: SS number, name, date of birth and address.

In summary, the Department of Income Maintenance has undertaken a major effort to plan numerous crossmatches. A major part of this process to plan for an evaluation of the cost effectiveness of these matches.

Very truly yours,

George B. Coleman
Deputy Commissioner

110 Bartholomew Avenue — Hartford, Connecticut 06115
An Equal Opportunity Employer

State of Mississippi

STATE DEPARTMENT OF PUBLIC WELFARE

P. O. Box 352
515 E. Amite Street
Jackson, Mississippi 39205

DR. DONALD B. ROARK
Commissioner

STATE BOARD
John G. Corlew, Pascagoula, Chairman
Jennie R. Walsh, Oxford
Jessie L. Weeks, Eupora
Willie J. Green, Heidelberg
Lamar Braxton, Natchez

9 35 DEC 27 '82

December 20, 1982

Mr. William S. Cohen, Chairman
Subcommittee on Oversight of
Governmental Management
Washington, D.C. 20510

Dear Mr. Cohen:

In response to your letter of November 8, 1982, we are submitting the following comments.

1. Types of matching:
    - A. Match of ADC eligibles with Employment Security Commission records. This match identifies individuals who have unreported earnings or unemployment benefits. This match is done quarterly.
    - B. Match of Mississippi ADC files with Illinois ADC files. This match is conducted semi-annually.
    - C. A monthly match with Medicaid files to determine individuals who are receiving SSI benefits and are not eligible for ADC benefits.
    - D. Interjurisdictional Match. This match is conducted by HHS and involves all states who wishes to participate.
2. Results of matching:
    - A. During the months of June and July, 1982 a total of 245 cases.of suspected fraud were reported due to this match. Overpayments totaled $111,392.00 for these two months. We do not know how much of this money will eventually be recovered nor have we estimated the savings because of the prevention of future overpayments. Recoupment from the check was initiated for 117 of these cases.
    - B. The last of these matches was completed in April 1982. There were 24 cases involving duplicate payments from both states. The estimated savings that has or will be achieved was not established.
    - C. A total of 152 possible SSI recipients were identified and 121 individuals removed from ADC during the months of July and August 1982. Estimated savings was not established.
    - D. This match identified 14 cases in Mississippi in which duplicate payments were received from another state. (This match is not completed) We have also referred 10 cases to other states for investigation of probable fraud and three cases of suspected fraud are being investigated within the state. In the past many of these cases have gone to court but we have ~~not~~ kept a record of the actual amount recovered.

3. Estimated costs of performing the matches:
   The costs of these matches is for the most part limited to computer time and worker's time reviewing records. We have not kept records on costs or savings because records on staff time have not been available. It seemed more important to prevent further overpayments and try to recover the overpayments that have been made than to spend time totaling costs and savings, estimating worker's time, and filling out reports. It appears obvious that there have been considerable savings.
4. See #2 above.
5. It seems that this should be left to the individual states. If certain types of matches are possible of which we are unaware then we should be notified of their availability and let us decide whether or not we wished to participate. There are probably numerous possibilities of matches that could be done but without staff to carry them out we need to be selective. Placing restrictions on what we can or cannot do does not seem to be the best of judgements. States have a better idea as to what will work for them. There has been much planning before hand on any matches that we have done. Only authorized persons have access to our findings and we are certainly aware of confidentiality and are not violating anyone's rights.
6. We seem to have had no problem so far in doing the matches that we have done.
7. We have policy written on this and we should assume that for the most part it is being followed. We do not know of any problems with this.

We do not currently have an automated system for the Food Stamp Program in this State; however, we have initiated wage match with Employment Security. Data is recorded manually at the county level and submitted to State Office where it is keypunched. Initial data indicates a substantial percentage of matches, but we do not have at this point sufficient data to determine the impact, i.e., the number of matches which indicate unreported income and the resulting amount of overissuance.

Beginning January 1, we plan to use our temporary automated system for wage match rather than having the counties manually prepare forms for keypunching in State Office. It is on this same day that the regulations mandate statewide crossmatch.

If you have further questions, please let us know.

Sincerely,

Donald B Roark

Donald B. Roark
Commissioner

DBR:ps

PRIVACY TIMES

Senator William S. Cohen
Chairman
Subcommittee On Oversight
Of Government Management
U.S. Senate
Washington, D.C. 20510

December 2, 1982

Dear Senator Cohen:

The enclosed articles from Privacy Times are submitted for inclusion in the Subcommittee's record relating to the computer matching hearings. These articles briefly touch on several of the important privacy issues that arise from computer matching. I also request that an article I published in the Washington Post, July 1, 1979, be included in the record.

As a journalist who has followed closely the development of computer matching projects, I would like to offer a few personal observations.

From a privacy perspective, computer matching poses several threats because it involves widespread sharing of personal data by federal and state agencies with little regard for Privacy Act restrictions. The current practice of justifying the transfer of personal records between agencies through the Privacy Act "routine use" exception appears to contradict congressional intent underlying that exception. The routine use clause permits transfer of records when such transfer is compatible with the purposes for which the data were collected. But it's fairly obvious, for instance, that data on railroad retirement recipients were not collected for the purposes of matching with AFDC file. In other words, the current practice constitutes an "end-run" around the Privacy Act. If we want the Privacy Act to have any meaning, it should be amended to cover computer matching.

The larger problem, however, concerns the lack of a federal privacy policy by the current Administration, and the absence of a permanent official body to monitor developments that could threaten privacy and articulate privacy interests. Unless this trend is reversed, the public's distrust for public and private institutions will grow because they realize their personal data is being manipulated without their informed consent.

As for computer matching, I urge you to be skeptical about its usefulness as it is currently practiced. Every time that an outsider has expended the time and energy to investigate an agency's claim that a given computer matching program has saved "millions of dollars," the investigation has proven the claims to be false. In some cases, the computer matching programs cost more than they saved. Meanwhile, data on thousands of individuals are used in ways that set dangerous precedents for personal privacy rights.

Sincerely Yours,

Evan Hendricks
Editor/Publisher

Privacy Times/ 2364 Champlain St. N.W., Washington, D.C. 20009 (202) 234-4813

PRIVACY TIMES

REPRINT FROM PRIVACY TIMES

DECEMBER 1, 1982

PRIVACY SAFEGUARDS SEEN LACKING IN FEDERAL COMPUTER MATCHING SPREE

The Reagan Administration's revision of computer matching guidelines has sparked a dramatic growth in matching programs, thus increasing the amount of personal data being shuffled and swapped by federal and state agencies. Critics complain this trend heightens the potential for privacy abuses. But the new guidelines, coupled with other Administration policies, removed the minimal privacy safeguards that were in place.

Last June, a few months after the guidelines were revised, an estimated 11 federal agencies were operating 90 matching projects in such areas as veterans, black lung, AFDC, railroad retirement and Medicare/Medicaid benefits.

Indications are that the number of matching projects continues to swell. Officials in various state and federal agencies are meeting full time to dream up new projects, according to the Long Term Computer Matching Project, a creature of the President's Council on Integrity and Efficiency. Made up of inspector generals, the President's Council "seeks to facilitate and encourage the use of computer matching and related techniques," in part by addressing "obstacles."

Its first step in achieving this goal was revision of guidelines drawn up by the Office of Management and Budget in 1979 as part of President Carter's national privacy policy. The Carter Administration was concerned about the privacy implications of unchecked matching, particular considering agencies' appetites for personal data. Although it did not directly restrict matching, the Carter Administration intended to control its growth by requiring agencies to demonstrate to OMB 60 days in advance that a proposed match would be "cost effective" and that the savings would outweigh potential threats to individual privacy rights.

The Carter guidelines recognized that matching posed an inherent threat to privacy and required agencies to prove the risk was worth it. Moreover, they gave OMB the responsibility of weighing the balance. "The old guidelines," said one OMB official, "got us into an intervenor position. If we thought any matching project was out of line, we could step in and block it." OMB did not stop one matching project under the guidelines, but some said its presence prompted agencies to think twice before proposing a match.

The revised guidelines, by removing the cost effectiveness test, took OMB out of the intervenor position and left matching policy to individual agencies, which now are being encouraged to match by the President's Council.

The result has been a computer matching "boom" featuring widespread comparisons of personal records held by different agencies. Due to technological advances, it is becoming possible to match nearly any data base held by federal or state agencies. AFDC, Food Stamp and Medicaid files are matched against workmen's compensation records, federal employee files are matched against those who owe money to the Farmers Home Administration and health professional receiving federal funds are matched against a list of overdue student loans. The key to nearly all matching efforts is the Social Security number.

Critics contend that matching contradicts the purposes of the Privacy Act: To allay citizens' fears that giving personal data to one agency meant that any other agency could get them, and to check the use of the Social Security number as a universal identifier.

MASSACHUSETTS WELFARE, BANK MATCH TARGET OF CLASS ACTION LAWSUIT

A massive computer match of Massachusetts welfare and bank records has led to the filing of a class action lawsuit charging that the state exceeded its authority and violated confidentiality provisions of welfare laws.

The suit, filed in federal court in Boston by the Massachusetts Law Reform Institute, challenged claims by the State Department of Public Welfare that the matching project was authorized by a 1967 state law. It charged that the state overstepped legal bounds by disclosing welfare recipients' Social Security numbers as the basis for the match.

U.S. District Judge David Mazzoni, although refusing to grant a temporary restraining order, is expected to begin hearing arguments in the case later this month.

The lawsuit coincided with growing evidence that the highly-touted matching program may turn out to be less productive than its proponents originally claimed. In the heat of tight Democratic primary race, Massachusetts Governor Edward King held a press conference in September to announce that a preliminary match with Boston-area banks turned up more than 3,000 recipients with bank assets exceeding legal limits (see Privacy Times, Oct. 6th).

Since then, however, sources have told Privacy Times that state welfare officials concede the program was hastily conceived and ill-prepared. Recipient records, they said, were not properly cleaned before the match -- prompting a preliminary number of "raw hits" that overstated the numbers who actually may have been violating the law.

One source asserted the match was a last-ditch effort by King to get favorable publicity before the Democratic primary, which he subsequently lost to Michael Dukakis. The source said King's actions raised the prospect that he manipulated personal files held by the state for his own gain.

Allan Rodgers, an attorney who brought the class action suit, acknowledged that a state law requires banks to inform the state welfare department, upon request, "the amount deposited. . . of a person named," who is receiving welfare. However, the state did not present banks with the names of welfare recipients; rather it forwarded their Social Security numbers and went beyond the law's authority, Rodgers claimed.

Rodgers also said the match was plagued by widespread error. Social Security numbers provided by banks had a 15 percent error rate, he said. When the state assembled its list of raw hits (those Social Security numbers which turned up on welfare and bank records), it failed to do further follow up. Instead, it simply sent notices to recipients informing them that they were cut off.

"The result was a 30 percent appeals rate -- six times the normal average," Rodgers said. "But since 70 percent of those who didn't appeal may be entitled to benefits, we filed suit."

Another problem, he continued, was the computer's inability to distinguish between different types of bank accounts.

"The typical case involved an elderly parent setting up a joint bank account with another family member who was on assistance. The parent usually controlled the account and often was the only person to make deposits. In some cases, the family member on assistance did not know that his or her name was on the account. But the parents set up joint accounts so that when they died, the money would go directly to the other family member," Rodgers said.

"So many of those nabbed by the computer were tied to these bank accounts in name only. But the computer had no way of knowing that," he said. (Lisa Lessard v. Spirito, et al.: USDC-Dist. of Mass.)

COMMENTS ON COMPUTER MATCHING

FROM JAN FREESE, DIRECTOR, SWEDISH DATA INSPECTION BD.
(PRIVACY TIMES, Sept. 22, 1982)

Freese is a strong advocate of the "omnibus" approach. When asked about the United States' approach of enacting different laws for separate kinds of personal records, he responded, "I never believed in that. With the merging of computers and record systems everything is just too complicated. The separate approach means that so much of what you want to protect falls between the cracks. It's easier to have an omnibus law that is practiced (implemented, in the right way."

He also is a strong opponent of "data linking," known here as computer matching. "When you merge two different records and create a new one you lose 'data quality.' That's because you're taking records that were created for different purposes and putting them together for still another purpose. It's like merging apples and pears!"

"Let's say you take a file that shows a man's taxable income and merge it with another of his files that shows his entire income. Both files may have been prepared for different purposes, but when you merge them together they both lose their meaning. Now a technocrat may think that this merging may help you find cheaters. But more often than not, they will only find shadows that make people look like cheaters because the data linking causes you to lose your data quality."

"And that's why," Freese said with a sigh, "it's easier to describe an elephant to a blind man than it is to explain privacy to a technocrat."

Testimony of David H. Flaherty on Matching Programs, for the U.S. Senate Committee on Governmental Affairs, Subcommittee on Oversight of Government Management, Washington, D.C., December 15-16, 1982

My name is David H. Flaherty. I am a professor of history and law at the University of Western Ontario, which is located in London, Canada. I welcome this opportunity to furnish the Subcommittee with written testimony about the privacy implications of computer matching programs and regret that I am unable to be present in person to answer your questions.

Perhaps I can begin with some background about my involvement with privacy-related matters. I have worked on aspects of privacy since I was introduced to the subject by Professor Alan F. Westin at Columbia University in 1964. My first book was an examination of the concept of personal privacy that existed in seventeenth and eighteenth-century America.[1] This interest reflects the fact that I am also a specialist in American history with a particular emphasis on social and legal history.

Since 1974 I have been directly involved in studying contemporary problems of data protection in Western Europe and North America. My 1979 book, Privacy and Government Data Banks. An International Perspective, looked at, in five countries, the problems of balancing the conflicting interests involved in the collection and use of personal information held by government agencies for research and statistical purposes.[2] There are a number of similarities between this problem and the balancing of interests that must take place in connection with matching programs.

Currently, I am the principal investigator of a three-year (1981-84) research project on "Data Protection Compared: an international perspective." In essence, I am taking a critical look at how data protection is working in practice in the public sector (and primarily at the national level) in the United States, Canada, the Federal Republic of Germany, France, Sweden, and the United Kingdom. My research is funded by the Ford Foundation and the Social Sciences and Humanities Research Council of Canada. Thus in the United States, for example, I am conducting research on the impact and operation of the Privacy Act of 1974. I am also trying to compare the efficacy of data protection at the federal level in the United States with the situation in other Western countries, which have created, or are in the process of creating, small government bureaucracies to implement data protection laws and to articulate privacy interests on a continuing basis. In my view the current U.S. federal system for data protection is seriously deficient.

1. The Goals of Matching Programs

It is worth remembering at the outset that matching programs originated during the administration of President Carter with the former HEW's "Project Match" in 1977.[3] The specific goals of attempting to remove fraud, waste, and abuse from government programs have thus been shared by the Carter and Reagan administrations. I should emphasize at the outset that I can only applaud these societal goals in the first instance, especially given the scope of government activities involved. As Inspector General Richard Kusserow of the Department of Health and Human Services noted at a meeting of the American Society of Access Professionals in Washington on November 18, 1982, his department has 5,000 computerized information systems, over 400 programs, and an annual budget in the neighborhood of $280 billion. This Inspector General has a staff of 1,000 to pursue the admirable goals of ending fraud, waste, and abuse. It is worth noting that a number of goals of the Inspector General "community" are identical to the aims of good data protection, especially the use of computer matching as an editing function to reduce data collection and to remove "pollution" in the form of inaccurate data from government personal information systems.

The President's Council on Integrity and Efficiency in government (PCIE), composed of sixteen Inspectors General, among others, reflects to a considerable extent the goals of the current administration. PCIE has developed some good practices in connection with matching programs that are in compliance with fair information practices, such as prohibiting any secret matches. As he stated during his November 18 presentation on computer matching, Mr. Kusserow and his associates are not insensitive to issues of personal privacy.

The problem in my view is that PCIE alone is incapable, even under the umbrella of the Privacy Act and the OMB Matching Guidelines, of balancing the sometimes conflicting interests of protecting the personal privacy of Americans versus its other goals, however laudable they may be in themselves. Competing values such as the privacy of individuals and the efficiency of government have to compete on an equal footing in order to achieve a satisfactory balance. What seems to be happening at present is that the people with a special mission to end fraud and waste are simultaneously trying, no doubt in good faith, to protect privacy interests.

As an historian with some perspective on the American past, perhaps I can be forgiven for suggesting that the current enthusiasm for matching programs strikes me as a typical search for a simple panacea for large problems that in some ways are almost hopeless. I would suggest, for example, that placing too great an emphasis on matching programs to solve the problems of the Social Security Administration is to slight the more fundamental problems that this particular agency is facing.[4]

2. Concern for Privacy in the United States

In simple terms, concern for personal privacy involves the desire of an individual to be left alone. Persons want to chose freely under what circumstances, and to what extent, they will expose themselves, their attitudes, and their behavior to others.[5] Two principal premises guiding privacy advocates are that privacy is not an absolute value, it is in competition with other important values in American society, and, secondly, that an individual in the late twentieth century can no longer adequately protect his or her own privacy without the assistance of data protection laws, and probably regulatory authorities, especially with respect to the public sector. In general, information furnished by individuals needs to be kept appropriately confidential in order for their personal privacy to be respected.

Although individuals will willingly give up a certain amount of personal privacy in return for obvious benefits, it seems to me unwise to suggest, as some have done, that more than a few individuals will completely sacrifice their personal privacy.[6] At the same time the general public is heavily dependent upon existing laws and specialized interest groups to ensure the protection of their privacy interests. This condition prevails in every Western nation. For an issue like matching programs, one cannot expect an avalanche of public opinion to stimulate Congress and civil libertarians to vigilance. In countries where data protection agencies exist, the legislature and the public can depend upon this specialized bureaucracy to exercise continuing oversight of privacy interests. No such responsible organization currently exists at the federal level in the United States.

Even if alarmist views about omniscient and omnipresent computers should and can be avoided, one cannot ignore the common situation in which the privacy implications of the use of a new technology, such as computer matching, are traditionally neglected in the rush towards "progress." New information technology usually is associated with the promotion of efficiency, which is clearly a very attractive goals for any government today. Yet the pursuit of efficiency and the suppression of fraud may not leave much room for consideration of such human values as privacy and confidentiality. This situation is independent of the rationale or the motivations prompting the development of such practices as matching programs; that the resulting capacity for surveillance or invasion of privacy is inadvertent does not mitigate the potential threat to the privacy interests of the citizenry.

3. Matching Programs under the Privacy Act of 1974 and the OMB Guidelines

3.1 The Privacy Act of 1974

In my view the Privacy Act of 1974 has been much abused in the development of rationales and justifications for matching programs since 1977. It is a mistaken notion that the Privacy Act was and is the last word in data protection, and that the privacy interests of citizens are safe so long as the Privacy Act's bastions are not openly breached. For its time this legislation was admirable and is comparable to landmark data protection legislation in Sweden (1973) and the West German Land of Hesse (1970). Many benefits have accrued to individuals under the Privacy Act, especially in terms of its primary focus on records management in the federal government. The provisions for facilitating access to one's own records has had particular benefits for federal employees. But Carole Parsons, formerly Executive Director of the Privacy Protection Study Commission, furnished a good summary of a fundamental criticism of the Privacy Act in a speech to a conference in Quebec City, Canada in May 1979: "The Privacy Act of 1974 is a landmark statute in many respects, but one of its most notable features is that it has little to do with protecting personal privacy in the traditional sense of guaranteeing an individual the right to be left alone...."[7] Parsons noted as an example that "the accounting of disclosures requirement... has turned out to be virtually useless."[8]

One problem with matching programs is that those seeking to justify them have looked to the letter, rather than to the spirit, of the Privacy Act. It is my contention that computer matching directly challenges Congressional findings about the need to protect personal privacy set forth at section 2(a) of the Privacy Act, and that the spirit, if not the letter, of computer matching is directly contrary to the intentions and aspirations of Members of Congress and the Senate as set forth in the Congressional Record and in the Legislative History of the Privacy Act. Instead of engaging in a detailed analysis of legislative history and intent, let me simply quote the following Congressional finding as stated in the Privacy Act: "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."[9] I shall argue that the same finding holds true today with respect to the practice of computer matching, and that Congress has a crucial responsibility to review the privacy aspects of matching programs, as you are doing here today.

3.2 The 1975 OMB Privacy Act Guidelines

The OMB guidelines of July 1 and November 21, 1975 on implementation of the Privacy Act have continued relevance today, since the OMB guidelines on matching programs of May 11, 1982 are expressly designed to be used in conjunction with them. Since the current guidelines seek to justify the transfer or release of personal information for matching purposes from one agency to another under the "routine use" provision of the Privacy Act, it is instructive to review what the 1975 basic guidelines said about routine uses: "One of the primary objectives of the Act is to restrict the use of information to the purposes for which it was collected."[10] The 1975 guidelines recognize that there are "corollary purposes...that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public."[11] Examples given in the guidelines of routine uses, as drawn from the Congressional Record, are described as "housekeeping measures." It is of course an open question whether the kinds of massive data transfers necessary for many matching programs fall under such an innocuous category. Furthermore, the 1975 OMB guidelines on implementation of the Privacy Act determine that "a 'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained:...."[12] Finally, the guidelines note that the requirement of a public notice by an agency for routine uses is intended "to deter promiscuous use of this concept."[13]

3.3 The OMB Guidelines on Matching Programs, 1978-1979

In response to pressing demands from the Carter Administration for guidance on computer matching, the OMB produced draft guidelines on matching programs dated August 2, 1978 and a final version on March 30, 1979.[14] Reporter Jake Kirchner of Computerworld has described in eloquent detail the frantic efforts made by administration lawyers, and even participants in the Carter Privacy Initiative, to find a justification for such practices as HEW's Project Match.[15]

One of the important aspects of emerging concern about matching programs and privacy in 1982 is that almost all of the privacy arguments were acknowledged at least in broad outline by various government agencies and the Carter Administration in the 1977-79 period.[16] OMB itself initially recognized the sensitive privacy elements of computer matching in the memorandum accompanying the draft guidelines of August 2, 1978: "...it is also clear that matching programs present the potential for significant invasions of personal privacy."[17] The significance of this statement lies in the fact that in later editions of its guidelines on matching programs OMB seems to have lost sight of this central privacy concern.

President Carter highlighted the guidelines on matching programs of March 30, 1979 as part of his Privacy Initiative. In submitting his legislative proposals to Congress, Carter made the following important statement about computer matching that is no less true today than when it was originally made: "...safeguards are needed to protect the privacy of the innocent and to ensure that the use of 'matching' is properly limited."[18]

In various specific ways the 1979 OMB guidelines on matching programs acknowledged the threat to personal privacy inherent in matching programs. In each of the two instances cited here, the actual language disappeared from the 1982 version of the same guidelines. Section 1 of the 1979 edition stated that "these guidelines are intended to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the individual's right to personal privacy." This of course remains the central issue facing agencies ultimately responsible for complying with the Privacy Act; the OMB's guidelines are only advisory and do not replace the terms of the statute itself. The 1979 guidelines also explicitly recognized the threat to privacy inherent in matching programs by making their utilization conditional upon a showing that "alternative means...would present a greater threat to personal privacy."[19]

The Carter Administration ultimately relied on the "routine use" provision of the Privacy Act to legitimize computer matching, relying on what Kirchner has aptly called "clever manipulation of [the] terminology of the law."[20] This reporter also states on the basis of documents to which he had access that "the government had known for years that use of the loophole for matching was, if not technically illegal, at least contrary to the spirit of the privacy law and the intent of its congressional sponsors."[21]

Various agencies at least initially balked at making their records available for Project Match, including the Civil Service Commission. CSC General Counsel Carl F. Goodman informed the acting deputy Inspector General of HEW that "it is evident that this information on employees was not collected with a view toward detecting welfare abuses." Goodman added that at the matching stage, "there is no indication whatsoever that a violation or potential violation of law has occurred."[22] When the Department of Defense finally decided that complying with Project Match could be construed as a new routine use, then-Representative Richardson Preyer, chairman of the House Government Information and Individual Rights Subcommittee, strongly protested to the Defense Secretary.[23]

The draft OMB guidelines of August 2, 1978 included some useful controls for the protection of privacy, which were unfortunately missing in an explicit fashion from the 1979 version:

> S. 3(g): The matching program should minimize the number and extent of the disclosures of information which pertain to identifiable individuals.
>
> S.5(b)(4): All routine uses permitting disclosures for matching programs should (a) be as specific and limited as possible.

Since Kirchner enjoyed access to materials on matching from 1977-1979 that are not otherwise publicly available, it is appropriate to close a discussion of this period by citing his summary judgment: "The intent of the guidelines, no doubt, was to forbid any computer matching program that could not be completely justified under the privacy law. The practical result of the guidelines, however, was in effect to authorize all manner of record disclosures for whatever reason might be conveniently labeled 'routine uses' by any agency wanting to perform a matching operation."[24]

3.4 The OMB Guidelines on Matching Programs, 1982

On May 11, 1982 OMB published "Revised Supplemental Guidelines for Conducting Matching Programs" that were more than fifty percent shorter than the 1979 edition. The stated purpose of the revision was updating, simplification, the reflection of experience, and the incorporation of agency recommendations for clarifications and changes. In addition to the criticisms I have already advanced of such matching guidelines, the 1982 version seems to place federal agencies in an almost impossible legal situation. Matching is to be done in compliance with the "provisions" of the various OMB guidelines and the Privacy Act.[25] It is arguable that it is impossible for an agency to release data for matching programs to another agency and to still comply with the Privacy Act: "Complying with these Guidelines...does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these Guidelines."[26] There is no existing mechanism whereby a federal agency can ascertain whether or not it is in compliance with the Privacy Act, short of responding to a criminal prosecution or a civil suit for engaging in a matching program.

The 1982 guidelines further provide that an agency can release personal information for matching programs to another agency, "if the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act...."[27] Internal dialogue within any such agency is almost inevitably much too one-sided for the adequate identification and protection of the privacy interests of the individuals thereby affected. Moreover, it is arguable that compliance with the Privacy Act itself is insufficient to protect personal privacy in a satisfactory manner, even if any one agency can hardly be held responsible for the deficiencies of this statute.

The 1982 OMB guidelines on matching programs are replete with conditions that place federal agencies in an ambiguous position in terms of compliance with the Privacy Act and in terms of protecting personal privacy in an acceptable manner. The articulation of privacy concerns in many parts of the guidelines seems to be largely pious language. For example, a source federal agency faces the burden of deciding whether to disclose personal records to another federal agency "to make sure they meet the necessary Privacy Act disclosure provisions...."[28] Furthermore, disclosure of records to a matching agency and disclosure of hits by a matching or source agency has to be done in accordance with paragraph (b) of the Privacy Act, which is a large, general paragraph.

This situation clearly indicates the consequences of the lack of an agency charged with monitoring compliance with the Privacy Act itself. OMB, even through its Office of Information and Regulatory Affairs, has no role under the 1982 matching guidelines. Moreover, the office in question is doing very little in practice about oversight of the Privacy Act. Even if any part of OMB was actively involved in measures for the protection of privacy in a meaningful fashion, this executive agency is too tied to the current political goals of any administration to be an ideal location for balancing privacy interests against other values.

3.5 Conclusions about the Guidelines on Matching Programs

1. As noted earlier, certain of the goals of matching programs are in conformity with the customary goals of good data protection, such as reducing the amount of personal information collected and ensuring its accuracy. The 1982 OMB guidelines on matching also include some good practical protections for personal privacy, including the requirements that only the minimum information necessary for a match should be disclosed, that there should be written agreements on data use, that there should be controls on the disposition and return of records, and that notices should be sent to the OMB and to Congress concerning the creation of new systems of records.[29]

The current matching guidelines do seem to exclude from their scope certain practices which are either neutral from the point of view of protecting privacy or deserve closer scrutiny on privacy grounds. In the first place there would appear to be no privacy grounds for questioning a match or audit that occurred in close proximity to the filing of an application by an individual for a benefit, since the person can be informed and should expect that such an audit will normally take place. Yet the OMB guidelines state that such an up-front audit is not a "matching program."[30] Secondly, the current guidelines only cover interagency matches, not ones internal to an agency.[31] Given the huge size of several federal agencies, it is presumptuous to suggest that internal matching programs do not pose privacy problems.

2. One of the fundamental problems with federal matching programs is that the sole measure of concern for privacy is the Privacy Act of 1974 and the 1975 OMB guidelines for its implementation rather than a more general conception and representation of the privacy interests of Americans. The questions and answers about computer matching issued by PCIE on July 1, 1982 discuss the protection of personal privacy solely in terms of compliance with the Privacy Act: "These provisions of law and the [OMB] guidelines protect individual privacy."[32]

In a presentation on computer matching to the American Society of Access Professionals on November 18, 1982, James Durnil, deputy assistant Inspector General for Audit at Veterans Affairs, stated that his office plans its matches in order to comply with the Privacy Act and the OMB matching guidelines. The Inspector General's office at Veterans Affairs wants to protect personal privacy, and its members are subject to penalties for violation of the Privacy Act. Durnil further stated that his office had never violated the Privacy Act. One response is that it would be very difficult for anyone, including an individual affected, to learn that a breach of the law had even occurred.

The key question for all Inspectors Generals is whether they have ever violated the privacy of individuals as opposed to violating the Privacy Act. Richard Kusserow of HHS stated during the ASAP meeting that his office was not invading anyone's privacy, which is of course possible. What seems to have received insufficient consideration from PCIE and the Inspectors General is the broad interests and values at stake when one is discussing the protection of personal privacy. The "we are not breaking the privacy act" syndrome is an unsatisfactory state of affairs.

3. The reliance on the concept of a "routine use" to legitimize matching programs seems contrary to the spirit and the guiding principles of the Privacy Act. At an ASAP session on November 19, 1982 Ronald L. Plesser, formerly general counsel of the Privacy Protection Study Commission, expressed his own doubts that Congress had ever intended such interpretations of routine use as those currently being employed. Plesser also stated on the basis of his own recent experience with litigation under the Privacy Act that the statute was almost unenforceable. This point has direct relevance to an evaluation of the adequacy of the current

enforcements mechanisms in criminal and civil law under the Privacy Act. A federal employee releasing records for a matching program to another agency might be subject to criminal penalties or a civil suit for failure to comply with the Privacy Act.[33] Yet another participant from the floor in the ASAP session remarked that the initial sensibilities of federal civil servants about the possibility of a prosecution or a law suit were greatly reduced after the passage of time demonstrated that such eventualities were very unlikely.

4. A final inadequacy of current matching programs and practices is that there is no established mechanism or forum whereby the conflicting interests inherent in such activities can be debated and balanced, which is a further reminder of the value of these Senate hearings. PCIE, for example, is an inappropriate locale for such deliberations, because of its central goals, however admirable they may be in themselves. It is equally questionable that OMB or any single federal agency is suitably informed to balance fully such competing interests as efficiency and privacy, especially in light of the vigorous efforts of Inspectors General and the Reagan Administration to end as much fraud and waste as possible.

Persons familiar with both matching programs and the Privacy Act argue that they want to allow the use of new technology and at the same time protect individual rights.[34] The question is how to achieve such laudable goals. There is probably little disagreement that computer matching should be carried out in such a manner as to pose as little challenge as possible to the privacy interests of the citizenry, but the issue remains of how best to do this. If one agrees that the indiscriminate use of matching is in no one's best interests, who is going to set the appropriate limits? These issues will be considered again below.

4. The Challenge of Matching Programs to Personal Privacy

4.1 Recognition of the Privacy Interests at Stake

Although one can readily understand an instinctive resistance to matching programs on grounds of concern for civil liberties, the objective threat of these measures to such values as personal privacy must be evaluated in concrete terms so as to avoid, among other things, a Luddite or an Orwellian mentality. The fundamental issue is identifying exactly what privacy interests need to be protected in the process of computer matching.

It is self-evident that identifying privacy interests is never an easy matter. One basic criticism of European data protection laws, for example, is that privacy interests are rarely defined in an adequate fashion, partly because it is so difficult to accomplish. In my view it is much too easy simply to assert, as the revised Swedish Data Act of 1982 continues to do, that data processing and record keeping should not cause "undue encroachment" upon the privacy of individuals. With respect to computer matching, in turn, one can reasonably ask whether a person's privacy is in fact invaded in any meaningful way, if his or her record in a federal information system is simply checked along with millions of others for compliance with a particular law? One possible answer is that an invasion of privacy only occurs if the data were not collected from individuals with such a purpose in mind.

Since the practice of matching records by computer is only about five years old at the federal level in the United States, one is largely left with the necessity of raising questions about how it might affect the privacy interests of individuals. Developing practices with respect to matching programs will more fully reveal the realities of the challenge, but they should be anticipated as much as possible in advance. What privacy interests are involved if matching occurs within a single file? Are different privacy challenges posed by matching programs that are recurring as opposed to single operations? Is the latter type of operation more likely to resemble an ill-conceived fishing expedition among personal records?

Consideration of general privacy interests at stake in matching programs can begin with the observation that individual claims to personal privacy are generally based upon a sense of morality as opposed to an expectation based solely on legislated rights to privacy. Protecting privacy in other words is not, and should not be, simply a question of law. In pursuing privacy principles in practice one can initially apply the precepts of the code of fair information practices that originated in the United States with the famous HEW report of 1973 and were subsequently enshrined in the Privacy Act.[35] Perhaps even more germane for current purposes are the important general principles highlighted in the 1977 Report of the Privacy Protection Study Commission. Two of them seem especially appropriate to a consideration of computer matching: minimizing intrusiveness in individual lives, and giving persons a legitimate expectation of confidentiality when they give up information about themselves for a particular purpose.[36]

4.2 Informed Consent For Data Transfers

One basic premise of fair information practices is that data should only be used for the purpose for which they were collected, unless the consent of the individual is obtained. Thus real privacy problems emerge when federal information systems are used for purposes that were in no way anticipated or announced at the time of data collection. Privacy advocate Robert Belair has recently stated with respect to intra-agency data sharing in the federal government that "this type of sharing threatens privacy interests by permitting the non-consensual sharing of subject information without notice to the subject."[37] He has further identified a subject's interest in prohibiting disclosures of data for compatible purposes:

> First, from a conceptual standpoint, it is not logical to conclude that because personal information is used for a purpose compatible with the purpose for which it was developed or collected, record subjects have no interest in contesting disclosure.... The disclosure

> of information to a new party, the passage of time, and changes in circumstances may all have the effect of making a "compatible" disclosure harmful to a subject's interests.[38]

4.3 The Handling of Hits in Matching Programs

Probably the most invasive aspect of matching programs is the follow-up of individuals who are identified by the matching process as "hits." The 1982 OMB guidelines define a "hit" as "the identification, through a matching program, of a specific individual."[39] If one seeks to argue that a computer running through a million records is only a minimal challenge to individual privacy interests, the harsh reality in terms of privacy is that the matching process ultimately leads to the targeting of specific persons for further contacts. This practice reveals one of the flaws in the PCIE argument that "computers are much less intrusive with regard to individual privacy than people."[40] It is obvious that such an assertion only tells part of the story.

A whole series of questions need to be answered from a privacy perspective about the handling of hits. How is the process handled? At what point is an individual "hit" actually approached? How is this handled? Is the approach done over the telephone or in person? Is the target summoned impersonally to present himself at a government office? Is the procedure accusatory or sensitive to individual rights? What are the emotional and psychological burdens for an individual of being identified by means of a "hit" as a target in a government investigation for fraud? How often is such an investigation inspired by an error that is no fault of the data subject? Could such a process unfairly jeopardize a subject by such means as investigative calls to an employer?

There is not yet enough evidence publicly available about experience with matching programs to furnish adequate answers to such questions. The basic fact, however, as PCIE has indicated, is that "raw hits have to be verified."[41] It is not clear whether or not the entire process depends upon direct contact with the hit, or whether further analysis of secondary data can be undertaken initially. The pursuit of hits that prove to be invalid or erroneous can be an invasion of the privacy of individuals in a very direct way. PCIE inadvertently makes this point in the following statement: "It should first of all be recalled that people who need assistance and legitimately apply for help are not the targets of matching and will not show up on match lists unless through error."[42] Further information about how the process is intended to work appeared in the Federal Register announcement of a proposed matching program between the Department of the Army and the City of New York. Readers are informed that "only the 'hits' will be turned over to personnel from the City of New York." There is no indication of whether or not these are raw hits or ones that have been initially investigated. The latter may be implied from the additional statement that "in those situations where there is any question as to eligibility, the recipient will be personally contacted to resolve the issue."[43]

It thus seems evident that the investigation of hits will involve a lot of direct contact with the individuals believed to be concerned. In the spring of 1979 a U.S. District Court judge in Massachusetts ordered a stop to interviews in response to a class action suit, after the state had interviewed 15,884 welfare receipients, who were identified as hits, and ordered them to prove their eligibility.[44]

The Office of the Inspector General for the Department of Health and Human Services has recently published three volumes of computer applications in matching programs, which have the incidental benefit of demonstrating how certain matches and follow-ups can involve sensitive matters. For the purpose of finding "illogical billing situations" involving physicians or health care providers, the IG's office has reviewed billing files on abortions and sterilizations. In the first instance HHS designed a computer application to identify billings for an abortion procedure where more than one claim was processed within a short period of time: "The program was run in one location. The results were turned over to program administrators for follow-up."[45] With respect to sterilization procedures, the goal is to make sure that claims were not processed for persons under twenty-one, since the individual has to have reached that age to obtain a government payment in this instance. The computer application identified claims for sterilization and related services, which obviously included all persons for whom billings had been submitted. The result was that "five hundred sterilization and related service claims were identified," and "claims totaling over $300,000 were referred to program administrators for follow-up."[46] One does not need to know much about the details of these particular matching programs to realize that very sensitive interests of relatively young persons are involved.

4.4 Restraining the Growth of Matching Programs

One of the critical issues associated with the regulation of computer matching is how to prevent its uncontrolled and unfettered growth. The practice raises again nascent fears about record linkages for good and bad purposes and the creation of a dossier society in which legitimate expectations of privacy will be difficult to achieve.

Perhaps the most demonstrable fear is that matching programs will lead to the creation of large new information systems for the purpose of ending fraud, abuse, and waste in government programs. There is some scattered evidence that this is actually happening. The Reagan Administration had a plan for a National Recipient Information System in HHS that would have included twenty-five million welfare recipients in an automated data base.[47] PCIE has issued assurances that no great master file in the hands of the government will result from computer matching.[48] But Richard Kusserow stated at the ASAP meeting in Washington on November 18 that Veterans Affairs was creating a national file of deceased individuals that should be available for government-wide use by March, 1983. Unless one accepts the unpalatable notion that dead persons have no further claims to personal privacy, the creation of such a large national data bank is a direct result of matching programs. Some matches also involve the use of the entire federal payroll. PCIE has further stated that "no permanent files identifying [hit] individuals result [from computer matching,] and therefore no master file can develop over time."[49] The same political pressures inspring matching programs may also lead to demands for a master file of "welfare cheats', so that they may be watched more easily.

PCIE has made the surprising claim that matching programs reduce the threat of government invasion of privacy, because the process uses "large, separate and disparate data bases and files."[50] Depending on one's perspective on these matters, it is the use of such disparate information systems that creates one of the challenges of matching programs to personal privacy. Massive amounts of personal information are involved. For example, the Social Security Administration's Title 2 Retirement, Survivors and Disability file, involving 350 reels of computer tape, was matched with a list of all persons dying in previous months obtained from the Health Care Financing Administration.[51]

The danger for privacy is that the preoccupation with government efficiency will lead to the national data bank mentality that Congress rejected with such enthusiasm during the mid-1960s. A national data bank would be or at least could be very efficient, but it would also further encourage the kind of society that Orwell warned us against. In fact, it is important to note that many of the initial concerns about matching programs revolved around images of a national data bank and the advent of Big Brother. In 1978 the Carter Administration recognized the risk that the public would begin to fear the creation of a national data bank.[52] In 1980 a spokesman for the Department of Defense stated that he was philosophically opposed to the use of computer matching to facilitate registration for Selective Service, because of the "Big Brother" tone of matching programs.[53] Inspector General Kusserow has publicly stated that he is anxious to avoid bringing on "Big Brother."[54]

4.5 The Limits of Matching Programs

The process of government would indeed be more efficient if we were all watched and monitored. What are the acceptable and tolerable limits of computer matching? The federal government could furnish everyone with a unique personal identifier or personal identification number, perhaps including a photograph, that would not suffer the limitations of Social Security Numbers. It could encourage every federal agency to build one central personal information system in order to encourage matching programs. One approaches the core values associated with personal privacy when one reflects on why some of these proposals seem unpalatable in American society. But how does one draw the line, and who should do so? How far afield can a federal agency legitimately go in testing for compliance with the eligibility requirements of a particular program? Should constraints exist against the matching of all records associated with any individual applying to the government for a benefit or payment? Should there be no restrictions on access to Internal Revenue Service or Bureau of the Census information systems? Should the government have access to individual bank accounts for matching purposes in order to reduce fraud, abuse and waste? It is obvious that a concern for privacy interests, among others, explains the fundamental resistance to such far-flung matching operations. Some routine uses of matching programs may be legitimate, such as for up-front auditing purposes, but most of us do not want to encourage the creation of total profiles for individuals, even within the confines of a particular agency.

5. Solutions

The Privacy Act of 1974 is in considerable need of revision during the 1980s to reflect more fully the challenges posed to personal privacy by new forms of information technology, including computer matching. The current mechanisms for regulating such programs as computer matching are totally inadequate for the protection of privacy. A revised Privacy Act could legitimize, regulate, and control matching programs and, ideally, set up a permanent mechanism for the articulation of privacy interests at the federal level. Like comparable data protection acts in Western European countries such as Sweden and the Federal Republic of Germany that have been or are currently being revised, the Privacy Act is a "first generation" statute that needs to be reviewed, revised, and strengthened. The common European solution to such problems of information technology as computer matching has been to create data protection agencies with a continuing mandate to represent the interests associated with personal privacy. Each of these existing agencies is currently struggling with the problem of matching programs, and it is never a foregone conclusion that the data protectors will prevail against other societal interests and agencies, including the legislature.

Canada, Sweden, France, and the Federal Republic of Germany, among other countries, have made provision for permanent organizations charged with data protection. The government of Margaret Thatcher is planning to introduce data protection legislation for both the public and private sectors in the current session of Parliament. The British system will include an independent Registrar of Data Bases and a staff of perhaps twenty non-civil servants with a continuing responsibility to oversee the development of information systems.

Data protection commissioners or agencies serve as an alarm system in connection with the protection of privacy. They exercise continuing oversight for privacy interests. They see to the implementation of the stated goals of data protection legislation. They investigate the degree of compliance with such laws through audits and security checks. They regulate specific national information systems in appropriate ways, largely through a process of mediation and the balancing of interests. They monitor and evaluate new technological developments in the information field, such as two-way cable television services, so-called smart cards, and matching programs. Each agency has specialists in various types of information systems and information flows, who can speak intelligently about data protection and security with the custodians of government information systems. Finally, each of these national agencies in Western Europe has been able to function successfully for as long as eight years with total staff sizes that remain under thirty-five persons.

A good data protection commission should have a statutory mandate and specified goals. It should have a Commissioner or permanent head and an advisory council. It should have as much independence of the executive and the legislature as possible under a particular constitutional system. A privacy protection agency only needs advisory powers in the public sector, since it normally enjoys ready access to the press and the legislature when non-compliance with data protection laws has been identified in a specific instance. Such an agency should engage in supervision, investigation, auditing, and advice giving. It can handle complaints from the general public about alleged breaches of data protection, engage in public relations activities, and help to shape new laws and regulations affecting information systems. Its most important duty is the articulation of privacy interests on a continuing basis.

Since matching programs pose at least some challenges to the privacy interests of every citizen, even if they have a beneficial deterrent effect in reducing fraud and waste, there is a fundamental need for the federal government to create a continuing mechanism whereby the privacy interests of individuals can be balanced against other societal values. The articulation of privacy interests could be done by PCIE, OMB, the courts, Congress, each federal agency, or ideally, a U.S. Privacy Protection Commission. There is a need to establish standards and limits on computer matching and then to enforce them. Inspector Generals have large staffs, approaching one thousand people in an agency like HHS, yet there is no permanent staff within the federal government with a broad mandate to seek to ensure the protection of personal privacy. At present, for example, there is little use in publishing notices of proposed matches in the Federal Register, since it is not read by the general public. A federal agency specifically charged with the protection of privacy could play a continuing role in the achievement of a successful balancing of the interests involved.

It is a tragedy that plans proposed by the Senate for a Privacy Protection Commission in the United States were not adopted at the time of the passage of the Privacy Act. It would be an appropriate celebration of 1984 for one to be created now.

Footnotes

1. David H. Flaherty, *Privacy in Colonial New England*, University Press of Virginia, Charlotteville, 1972.

2. David H. Flaherty, *Privacy and Government Data Banks. An International Perspective*, Mansell, London, U.K., 1979.

3. The early history of matching programs is treated in the excellent article by Jake Kirchner, "Privacy. A History of Computer Matching in the Federal Government," *Computerworld*, Dec. 14, 1981, In Depth, pp. 1-16.

4. See Peter G. Peterson, "Social Security: The Coming Crash," *The New York Review of Books*, XXIX, No. 19, Dec. 2, 1982, pp. 34-38.

5. See Alan F. Westin, *Privacy and Freedom* (New York, 1967), p. 7.

6. Compare the interview with the Japanese computer expert, Yoneji Masuda, in *Computerworld*, June 14, 1982, In-Depth, p. 11.

7. Carole Parsons, "Data Processing and the Right to Privacy," in International Conference on the Future of Public Administration, *Conference Proceedings*, vol. 9, p. 1906, Ecole nationale d'administration publique, Quebec, May 27-31, 1979.

8. *Ibid*., p.1919.

9. Privacy Act, 1974, s. 2(2).

10. *Federal Register*, vol. 40, No. 132, July 9, 1975, p. 28953.

11. *Ibid*., italics added.

12. *Ibid*.

13. *Ibid*.

14. "Privacy Act of 1974: Supplemental Guidance for Marching Programs," OMB, August 2, 1978; "Guidelines for the Conduct of Matching Programs," OMB, March 30, 1969.

15. Kirchner, *Computerworld*, December 14, 1981, In-Depth, p. 2

16. See Kirchner, *Ibid*.

17. OMB Guidelines, August 2, 1978, p. 2.

18. *Computerworld*, April 23, 1979, p. 13.

19. OMB Guidelines, March 30, 1979, s. 5(a).

20. Kirchner, Computerworld, December 14, 1981, In-Depth, p. 6.

21. Ibid., p. 3.

22. Quoted in ibid., pp. 6-7.

23. The letter is quoted in ibid., p. 7.

24. Ibid., p. 15

25. Office of Management and Budget, "Revised Supplemental Guidance for Conducting Matching Programs," Memorandum, May 11, 1982, s.5(a).

26. Ibid., s.1.

27. Ibid., s.5(a).

28. Ibid., s. 5(a)(1).

29. Ibid., sections 5(a)(2), 5(b), 5(d), and 5(e)(2).

30. Ibid., s. 4(c)(2)(3).

31. A point made by Hugh O'Neill of the Department of Health and Human Services at a session on computer matching, American Society of Access Professionals, Washington, D.C., Nov. 18, 1982.

32. PCIE, "Questions on Computer Matching," July 1, 1982, question 11.

33. Privacy Act, s. i(1), s. (g)(D).

34. Hugh O'Neill, HHS, in an ASAP presentation, Nov. 18, 1982.

35. Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Department of Health, Education and Welfare, Washington, D.C., 1973.)

36. Personal Privacy in an Information Society. The Report of the Privacy Protection Study Commission (Washington D.C., 1977), pp. 15-21.

37. Robert R. Belair, "Information Privacy," in Helen A. Shaw, ed., Issues in Information Policy (National Telecommunications and Information Administration, Washington, D.C., 1981), p.44.

38. Ibid., p. 48.

39. OMB Guidelines, 1982, s. 4(f).

40. PCIE, "Questions on Computer Matching," July 1, 1982, question 13.

41. *Ibid.*, question 6.

42. *Ibid.*, question 10; italics added.

43. *Federal Register*, vol. 47, No. 119, June 21, 1982, p. 26686.

44. *Computerworld*, May 7, 1979, p.19.

45. Department of Health and Human Services, Office of Inspector General, *Computer Applications*, Volume 1, *Health Provider Fraud and Abuse* (June, 1982), p. I-40.

46. *Ibid.*, I, p. I-41.

47. See *Computerworld*, XV, No. 19, May 11, 1981, pp. 1, 6.

48. PCIE, "Questions about Matching," July 1, 1982, question 12.

49. *Ibid.*

50. *Ibid.*, question 13.

51. *Computerworld*, XVI, No. 10, March 8, 1982, p. 35.

52. See Kirchner, *Computerworld*, December 14, 1981, In-Depth, p. 14.

53. *Computerworld*, Feb. 4, 1980, p. 5.

54. ASAP presentation, Washington, D.C., Nov. 18, 1982.